IV. *On the Residues of Powers of Numbers for any Composite Modulus, Real or Complex.*

By Geoffrey T. Bennett, *B.A.*

Communicated by Professor Cayley, *F.R.S.*

Received April 8,—Read May 5, 1892.

The present work consists of two parts, with an appendix to the second. Part I. deals with real numbers, Part II. with complex.

In the simple cases when the modulus is a real number, which is an odd prime, a power of an odd prime, or double the power of an odd prime, we know that there exist primitive roots of the modulus; that is, that there are numbers whose successive powers have for their residues the complete set of numbers less than and prime to the modulus. A primitive root may be said to generate by its successive powers the complete set of residues. It is also known that, in general, when the modulus is any composite number, though primitive roots do not exist, there may be laid down a set of numbers which will here be called *generators,* the products of powers of which give the complete set of residues prime to the modulus.

The principal object of Part I. is to investigate the relations which must subsist among any such set of generators; to determine the most general form that they can take; to show how to form any such set of generators, and conversely to furnish tests for the efficiency, as generators, of any given set of numbers. Other results which are obtained as instrumental in effecting these objects, such as the determination of the number of numbers that belong to any exponent, may also possess independent interest.

The object of Part II. is to make, for complex numbers, an investigation which shall be as nearly as possible parallel to that of Part I. for real numbers. Much of the work of Part I. may be applied immediately to complex numbers; of the rest some will need slight modification, and some will need replacing by propositions leading to corresponding results. Of those cases which thus call for independent treatment, the most noticeable is that of the modulus $(1 + i)^{\lambda}$, which is the complex analogue of the real modulus 2^{λ}.

The work is put in the form of a series of propositions, and is started almost from first principles. The early part is consequently elementary, but the advantages of completeness and ease of reference may be more than sufficient to compensate for this. A large number of illustrative examples are given. These will sometimes, perhaps, assist in elucidating the symbolical proofs which they follow; in all cases they will help to maintain clearly the actual arithmetical meaning of the results arrived at, a meaning which may easily seem obscure if it be noticed only in its symbolical and generalised form.

The Appendix contains tables of indices for complex numbers for all moduli whose norms do not exceed 100.

PART I.—ON THE RESIDUES OF POWERS OF NUMBERS FOR ANY COMPOSITE REAL MODULUS.

In what follows (except when the contrary is explicitly stated) we shall be treating of the residues of powers of numbers which are *prime* to the modulus with regard to which those residues are taken; and the modulus will be taken to be any composite number whatever. In this first part, moreover, all the numbers dealt with are real.

(1.) The residues (modulus m) of the successive powers of a number a prime to m form a recurring series of periods of terms, the first period beginning with the first term.

Consider the series of numbers

$$a,\ a^2,\ a^3 \ldots$$

Since a is prime to m, therefore any power of a is prime to m, and therefore the residue of a^s for modulus m is prime to m.

Hence each term of the series of residues,

$$a,\ a^2,\ a^3 \ldots \pmod{m},$$

is one of the numbers less than m and prime to it.

There are $\phi(m)$ numbers less than m and prime to it.

Hence in the above infinite series there are only $\phi(m)$ *different* terms.

Suppose that the first term which occurs for the second time is $a^{t+s} \pmod{m}$, and suppose that this is congruent to a^s.

Then

$$a^{t+s} \equiv a^s \pmod{m},$$

where s and t are both to have as small values as possible.

$$a^s(a^t - 1) \equiv 0 \pmod{m},$$

and since a^s is prime to m,

$$a^t - 1 \equiv 0 \pmod{m},$$

and so

$$a^{t+\sigma} \equiv a^\sigma \pmod{m},$$

for *every* value of σ

Hence the term which first appears a second time is the first term a; which appears next as a^{t+1}, t being the least number for which

$$a^t \equiv 1 \pmod{m}.$$

Definition.—The smallest number t which makes $a^t \equiv 1 \pmod{m}$, where a is prime to m, is called the *exponent* of a for modulus m. CAUCHY uses the word "*indicator*" in the same sense. He also uses "*maximum indicator*" to denote what will be called the *highest exponent*.

Thus the infinite series of residues of a, a^2, a^3, . . . consists of a repetition of the period of t terms beginning from the first term.

(2.) If t be the exponent of a and $a^s \equiv 1 \pmod{m}$ then t divides s.

Let

$$s = qt + r \text{ where } r < t.$$

Then

$$a^s = a^{qt+r} \equiv 1 \pmod{m},$$
$$(a^t)^q \,.\, a^r \equiv 1 \pmod{m},$$
$$a^r \equiv 1 \pmod{m},$$

whereas t is the smallest value (not zero) which makes $a^t \equiv 1$. Therefore

$$r = 0,$$

therefore

$$t \text{ divides } s.$$

(3.) FERMAT'S *Theorem.*

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

Let a_1, a_2, a_3, . . . $a_{\phi(m)}$ be the $\phi(m)$ numbers less than m and prime to it.

Take any one of them a.

Then since aa_1, aa_2, aa_3, . . . $aa_{\phi(m)} \pmod{m}$ are all prime to m, and no two congruent, they must be the same set of numbers as a_1, a_2, . . . $a_{\phi(m)}$; therefore

$$a_1 a_2 a_3 \ldots a_{\phi(m)} a^{\phi(m)} \equiv a_1 a_2 \ldots a_{\phi(m)} \pmod{m},$$

and, therefore,

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

Corollary.—It follows from this proposition and proposition (1) that the exponent of any number (modulus m) is always a divisor of $\phi(m)$. The propositions which follow will determine that divisor.

(4.) If t be the exponent of a then the exponent of a^s is τ: where $t = \kappa\tau$ and κ is the G.C.M. of s and t.

Let T be the exponent of a^s.

We have

$$a^t \equiv 1 \pmod{m},$$

therefore

$$a^{\kappa\tau} \equiv 1 \pmod{m},$$

$$a^{\kappa\sigma\tau} \equiv 1 \pmod{m},$$

$$(a^s)^\tau \equiv 1 \pmod{m},$$

therefore

$$\mathrm{T} \text{ divides } \tau. \quad \text{(Prop. 2.)}$$

Again,

$$(a^s)^{\mathrm{T}} \equiv 1 \pmod{m},$$

therefore

$$a^{s\mathrm{T}} \equiv 1 \pmod{m},$$

therefore

$$t \text{ divides } s\mathrm{T},$$

therefore

$$\kappa\tau \text{ divides } \kappa\sigma\mathrm{T},$$

therefore

$$\tau \text{ divides } \sigma\mathrm{T},$$

therefore

$$\tau \text{ divides } \mathrm{T},$$

therefore

$$\mathrm{T} = \tau.$$

Example.—The exponent of 3 for modulus 308 is 30: the residues of its successive powers are given in the following table:—

Number . . .	3	9	27	81	243	113	31	93	279	221
Power of 3 . .	1	2	3	4	5	6	7	8	9	10
Exponent . .	30	15	10	15	6	5	30	15	10	3

Number . . .	47	141	115	37	111	25	75	225	59	177
Power of 3 . .	11	12	13	14	15	16	17	18	19	20
Exponent . .	30	5	30	15	2	15	30	5	30	3

Number . . .	223	53	159	169	199	289	251	137	103	1
Power of 3 . .	21	22	23	24	25	26	27	28	29	30
Exponent .	10	15	30	5	6	15	10	15	30	1

where the exponents are all immediately deducible from the proposition.

(5.) The exponent of a is t and of a' is t' and t and t' are co-prime; then the exponent of aa' is tt'.

Let T be the exponent of aa'.

Then,

$$a^{t} \equiv 1 \pmod{m} \qquad a'^{t'} \equiv 1 \pmod{m},$$

therefore

$$a^{tt'} \equiv 1 \pmod{m} \qquad a'^{tt'} \equiv 1 \pmod{m},$$

therefore

$$(aa')^{tt'} \equiv 1 \pmod{m},$$

therefore

$$\text{T divides } tt'. \quad \text{(Prop. 2.)}$$

Again,

$$(aa')^{\mathrm{T}} \equiv 1 \pmod{m},$$
$$(aa')^{\mathrm{T}t} \equiv 1 \pmod{m},$$
$$a'^{\mathrm{T}t} \equiv 1 \pmod{m},$$

therefore

$$t' \text{ divides T}t \text{ (Prop. 2)},$$

therefore

$$t' \text{ divides T}.$$

Similarly,

$$t \text{ divides T},$$

and therefore (since t and t' are co-prime),

$$tt' \text{ divides T},$$

therefore

$$\mathrm{T} = tt'.$$

Corollary.—It follows that if the numbers $a, a', a'', \ldots$ have exponents (for modulus m) $t, t' t'', \ldots$ these exponents being all co-prime, then the exponent of $aa'a'' \ldots$ is $tt't'' \ldots$

Example.—The exponent of

23 mod 308 is 6; (23. 221. 155. 177. 67. 1),

and the exponent of

113 mod 308 is 5; (113. 141. 225. 169. 1).

Since 5 and 6 are co-prime, it follows that the exponent of

$$135 \equiv 23.\ 113 \text{ is } 30.$$

Corollary. *Example.*—The exponent of

$$\left.\begin{array}{l}111 \text{ is } 2\\ 221 \text{ is } 3\\ 113 \text{ is } 5\end{array}\right\}\text{therefore the exponent of } 111.\ 221.\ 113 \equiv 3 \text{ is } 30.$$

(6.) Let a have exponent t and a' exponent t' and suppose that t and t' are not co-prime. Then, if t and t' contain no prime factor raised to the same power in both, the exponent of aa' is the L.C.M. of t and t'.

Let

$$\left.\begin{array}{r}t = \kappa\tau\\ t' = \kappa\tau'\end{array}\right\}\text{where } \tau \text{ and } \tau' \text{ are co-prime,}$$

then

$$a^{\kappa} \text{ has exponent } \tau \text{ (Prop. 4),}$$

$$a'^{\kappa} \text{ has exponent } \tau' \text{ (Prop. 4),}$$

therefore,

$$(aa')^{\kappa} \text{ has exponent } \tau\tau' \text{ (Prop. 5).}$$

So if aa' has exponent T, then

$$\frac{\mathrm{T}}{\kappa} = \frac{\tau\tau'}{z}$$

where $\tau\tau'$ divides T, z divides κ and z is prime to $\tau\tau'$. (Prop. 4.)

Now since t and t' contain no prime raised to the same power in each, therefore $\tau\tau'$ contains every prime factor which occurs in t and t' and therefore contains every prime factor which occurs in κ. Hence z cannot divide κ and be prime to $\tau\tau'$ unless it be unity.

Therefore,

$$\mathrm{T} = \kappa\tau\tau' = \text{L.C.M. of } t \text{ and } t'.$$

(7.) If a has exponent t, a' has exponent t', a'' — t'', &c., for modulus m, and if, of the $tt't''\ldots$ numbers $a^r a'^{r'} a''^{r''}\ldots$ (mod m) formed by giving to r all values modulus t, to r' all values modulus t' . . ., no two are congruent; and if

$$a^s a'^{s'} a''^{s''} \ldots \equiv 1 \pmod{m};$$

then we must have

$$a^s \equiv 1, \quad a'^{s'} \equiv 1, \quad a''^{s''} \equiv 1, \ldots \pmod{m}.$$

For suppose that at least one of these congruences is violated.

Say

$$a^s \not\equiv 1 \pmod{m},$$

and, therefore,

$$s \not\equiv 0 \pmod{t}.$$

Then, because

$$a^s a'^{s'} a''^{s''} \ldots \equiv 1 \pmod{m},$$

therefore (multiplying by a^{t-s}),

$$a^t a'^{s'} a''^{s''} \ldots \equiv a^{t-s} \pmod{m},$$

or

$$a^0 a'^{s'} a''^{s''} \ldots \equiv a^{t-s} \pmod{m},$$

or

$$a^0 a'^{s'} a''^{s''} \ldots \equiv a^{t-s}\, a'^0 a''^0 \ldots \pmod{m},$$

which is contrary to the supposition that no two numbers of the form $a^r a'^{r'} \ldots$ (mod m) are congruent; for the last congruence obtained shows that if we make

$$\left.\begin{matrix} r = 0 & r' = s' & r'' = s'' \ldots \\ r = t - s & r' = 0 & r'' = 0 \ \ldots \end{matrix}\right\}$$

where

$$t - s \not\equiv 0 \pmod{t},$$

the two numbers are congruent.

Hence, we must have

$$s \equiv 0 \pmod{t},$$

and, therefore,

$$a^s \equiv 1 \pmod{t}.$$

Similarly,

$$a'^{s'} \equiv 1 \pmod{t'}, \text{ \&c.}$$

Definition.—If a, a', a'' . . . have exponents t, t', t'', . . . and if no two of the $tt't''$ . . . numbers that can be formed by products of their powers are congruent modulus m (as in the last proposition), then these numbers, a, a', a'', . . . which generate the $tt't''$ . . . incongruent numbers, will be called *independent* generators.

The last proposition may then be stated thus :—If a product of powers of a set of independent generators be congruent to unity, then each of those powers is itself congruent to unity.

(8.) If a, a', a'', . . . independent generators, have exponents t, t', t'', . . . then the exponent of $aa'a''$ . . . is the L.C.M. of t, t', t'' . . .

Let T be the L.C.M. of t, t', t'', . . . and τ the required exponent of $aa'a''$ . . .

$$a^t \equiv 1 \pmod{m},$$

therefore,

$$a^{\mathrm{T}} \equiv 1 \pmod{m}.$$

Similarly,

$$a'^{\mathrm{T}} \equiv 1 \pmod{m}, \text{ \&c.,}$$

therefore,

$$(aa'a'' \ldots)^{\mathrm{T}} \equiv 1 \pmod{m},$$

therefore,

$$\tau \text{ divides T.} \quad \text{(Prop. 2.)}$$

Again,

$$(aa'a'' \ldots)^{\tau} \equiv 1 \pmod{m},$$

therefore,

$$a^{\tau}a'^{\tau}a''^{\tau} \ldots \equiv 1 \pmod{m},$$

therefore,

$$\left.\begin{array}{l}\tau \equiv 0 \pmod{t} \\ \tau \equiv 0 \pmod{t'} \\ \tau \equiv 0 \pmod{t''}\end{array}\right\}\text{(Prop. 7)},$$

therefore,

$$\text{T divides } \tau,$$

therefore,

$$\mathrm{T} = \tau.$$

Corollary.—If the exponents t, t', t'', be all of them powers of the same prime, and a, a', a'', . . . are independent generators, then the exponent of the product $aa'a''$ . . . is equal to the greatest of the exponents t, t,' t'' . . .

(9.) If the exponent of a for modulus m is t, and for modulus n is t', and if m and n are co-prime, then the exponent of a for modulus mn is the L.C.M. of t and t'.

Let $t'' = t\tau = t'\tau'$ where τ and τ' are co-prime, so that t'' is the L.C.M. of t and t'.

Let the exponent of a for modulus mn be T.

Thus we have

$$a^{t} \equiv 1 \pmod{m},$$

and, therefore, raising to the power τ,

$$a^{t''} \equiv 1 \pmod{m}.$$

Similarly,

$$a^{t''} \equiv 1 \pmod{n},$$

and, therefore (since m and n are co-prime),

$$a^{t''} \equiv 1 \pmod{mn},$$

therefore

$$\text{T divides } t''. \quad \text{(Prop. 2.)}$$

Again,

$$a^{\mathrm{T}} \equiv 1 \pmod{mn},$$

therefore

$$a^{\mathrm{T}} \equiv 1 \pmod{m},$$

therefore

$$t \text{ divides T.}$$

Similarly,

$$t' \text{ divides } \mathrm{T},$$

therefore

$$t'' \text{ divides } \mathrm{T}.$$

Therefore

$$\mathrm{T} = t''.$$

Corollary.—If the exponents of a for moduli $m, m', m'', \ldots$ are respectively $t, t', t'', \ldots$ and the moduli are co-prime, then the exponent of a for modulus $mm'm'' \ldots$ is the L.C.M. of $t, t', t'' \ldots$

Examples.—The exponent of

$$\left.\begin{array}{l} 3 \text{ for mod } 4 \text{ is } 2 \\ 3 \text{ for mod } 7 \text{ is } 6 \\ 3 \text{ for mod } 11 \text{ is } 5 \end{array}\right\} \qquad \begin{array}{l} (3.\ 1.) \\ (3.\ 2.\ 6.\ 4.\ 5.\ 1.) \\ (3.\ 9.\ 5.\ 4.\ 1.) \end{array}$$

Therefore the exponent of

$$3 \text{ for mod } 4.\ 7.\ 11 = 308 \text{ is } 30.$$

The exponent of

$$\begin{array}{ll} 5 \text{ for mod } 4 \text{ is } 1. & \\ 5 \text{ for mod } 7 \text{ is } 6 & (5.\ 4.\ 6.\ 2.\ 3.\ 1.) \\ 5 \text{ for mod } 11 \text{ is } 5 & (5.\ 3.\ 4.\ 9.\ 1.) \end{array}$$

and, therefore, the exponent of

$$5 \text{ for mod } 308 \text{ is } 30.$$

The exponent of

$$\begin{array}{ll} 9 \text{ for mod } 4 \text{ is } 1. & \\ 9 \text{ for mod } 7 \text{ is } 3 & (2.\ 4.\ 1.) \\ 9 \text{ for mod } 11 \text{ is } 5 & (9.\ 4.\ 3.\ 5.\ 1.) \end{array}$$

and, therefore, the exponent of

$$9. \text{ mod } 308 \text{ is } 15.$$

(10.) If the exponent of a is t, and $t = pqr \ldots$ where p, q, r are co-prime factors of t, to express a as a product of numbers whose exponents are $p, q, r \ldots$

Let

$$\left.\begin{array}{l} \mathrm{P} \equiv 0 \ (\text{mod } qr \ldots) \\ \phantom{\mathrm{P}} \equiv 1 \ (\text{mod } p) \end{array}\right\} \quad \left.\begin{array}{l} \mathrm{Q} \equiv 0 \ (\text{mod } pr \ldots) \\ \phantom{\mathrm{Q}} \equiv 1 \ (\text{mod } q) \end{array}\right\} \ \&\text{c.}$$

These congruences determine one value each and one only (mod t) for P, Q, . . .

$$\begin{array}{l} a^{\mathrm{P}} \text{ has exp } p \text{ (Prop. 4)}, \\ a^{\mathrm{Q}} \quad ,, \quad ,, \quad q \\ \quad \&c. \end{array}$$

From the above congruences we obtain

$$\begin{aligned} \mathrm{P} &\equiv 1 \pmod{p}, \\ \mathrm{Q} &\equiv 0 \pmod{p}, \\ \mathrm{R} &\equiv 0 \pmod{p}, \\ &\&c. \end{aligned}$$

therefore, by addition,

$$\mathrm{P} + \mathrm{Q} + \mathrm{R} + \ldots \equiv 1 \pmod{p}.$$

Similarly,

$$\mathrm{P} + \mathrm{Q} + \mathrm{R} + \ldots \equiv 1 \pmod{q},$$

&c.,

and, therefore, since p, q, r, . . . are co-prime,

$$\mathrm{P} + \mathrm{Q} + \mathrm{R} + \ldots \equiv 1 \pmod{t},$$

therefore

$$a^{\mathrm{P}}.\, a^{\mathrm{Q}}.\, a^{\mathrm{R}} \ldots \equiv a \pmod{m}.$$

And so a is expressible (in one way only) as the product of numbers a^{P}, a^{Q} . . . whose exponents are p, q . . .

Example.—3 has exponent 30 mod 308.

To express it as a product of 3 numbers with exponents 2. 3. 5,

$$\begin{array}{lll} \mathrm{P} \equiv 0 \pmod{15} & \mathrm{Q} \equiv 0 \pmod{10} & \mathrm{R} \equiv 0 \pmod{6} \\ \quad \equiv 1 \pmod{2} & \quad \equiv 1 \pmod{3} & \quad \equiv 1 \pmod{5}, \end{array}$$

therefore

$$\mathrm{P} = 15 \qquad \mathrm{Q} = 10 \qquad \mathrm{R} = 6,$$

and, therefore,

$$3 \equiv 3^{15}.\, 3^{10}.\, 3^{6} \equiv 111.\ 221.\ 113 \pmod{308}$$

where

$$\left.\begin{array}{l} 111 \text{ has exp } 2 \\ 221 \quad ,, \quad ,, \quad 3 \\ 113 \quad ,, \quad ,, \quad 5 \end{array}\right\}$$

Similarly 79 has exponent 30 (mod 308), and

$$79 \equiv 79^{15}.\, 79^{10}\ 79^{6} \equiv 43.\ 177.\ 141 \pmod{308}$$

where

$$\left.\begin{array}{rl} 43 & \text{has exp } 2 \\ 177 & \text{,, ,, } 3 \\ 141 & \text{,, ,, } 5 \end{array}\right\}$$

(11.) The number of numbers that belong to any exponent t when the modulus is a prime p is $\phi(t)$.

If there are any numbers which have exponent t, mod p, let α be one.

Then because

$$\alpha^t \equiv 1 \pmod{p},$$

therefore each of the t incongruent numbers

$$\alpha, \alpha^2, \alpha^3, \ldots \alpha^t$$

when raised the t^{th} power is $\equiv 1$.

Hence each is a root of $x^t \equiv 1 \pmod{p}$ which has only t incongruent roots.

Therefore every number β which has exponent t, and which is therefore such that $\beta^t \equiv 1$ is included in the above set. Hence every number with exponent t is to be found in the above set. Now, of the powers of α there are $\phi(t)$ which have their index prime to t, and which, therefore, have exponent t (Prop. 4).

Therefore if there is *one* number with exponent t there are $\phi(t)$, and no more.

Now if $t_1, t_2, \ldots,$ are all the divisors of $p-1$, and, therefore, all possible exponents (Prop. 3, corollary),

$$\phi(t_1) + \phi(t_2) + \ldots = \phi(p).$$

Corresponding to each value t there are either $\phi(t)$ numbers or none with t as exponent. The number of numbers altogether is $\phi(p)$. Hence in no case can there fail to be $\phi(t)$ numbers with exponent t.

Corollary.—In particular there are $\phi(p-1)$ numbers with exponent $p-1$, modulus p, *i.e.*, any odd prime p has $\phi(p-1)$ primitive roots.

(12.) The exponents to which a number a belongs for successive powers of a prime p as moduli.

We suppose that a is prime to p and that $p \neq 2$.

Let the exponents to which a belongs for the moduli $p, p^2, p^3, \ldots p^\lambda \ldots$ be $t_1, t_2, t_3, \ldots$ respectively.

Then because

$$a^{t_{\lambda+1}} \equiv 1 \pmod{p^{\lambda+1}},$$

therefore

$$a^{t_{\lambda+1}} \equiv 1 \pmod{p^\lambda},$$

therefore

$$t_\lambda \text{ divides } t_{\lambda+1}. \quad \text{(Prop. 2.)}$$

Again

$$a^{t_\lambda} \equiv 1 \pmod{p^\lambda},$$

therefore (raising to the p^{th} power $a^{t_\lambda} = 1 + \kappa p^\lambda$)

$$a^{pt_\lambda} \equiv 1 \pmod{p^{\lambda+1}},$$

therefore

$$t_{\lambda+1} \text{ divides } pt_\lambda. \quad \text{(Prop. 2.)}$$

It follows from these two results that either $t_{\lambda+1} = t_\lambda$ or $t_{\lambda+1} = pt_\lambda$.

Each exponent in the series $t_1, t_2, \ldots t_\lambda, \ldots$ is either equal to that immediately preceding it or is p times that value.

We can show, however, that after the first set of equal exponents $t_1 = t_2 = \ldots$ comes to an end, that each exponent is p times that which immediately precedes it.

For suppose that, if possible, after

$$t_{\lambda+1} = pt_\lambda$$

we can have

$$t_{\lambda+2} = t_{\lambda+1}.$$

We thus have

$$t_{\lambda+2} = t_{\lambda+1} = pt_\lambda.$$

Now

$$a^{t_\lambda} \equiv 1 \pmod{p^\lambda} = 1 + xp^\lambda + yp^{\lambda+1},$$

say, where $x < p$.

Also,

$$a^{pt_\lambda} = a^{t_{\lambda+2}} \equiv 1 \pmod{p^{\lambda+2}},$$

therefore

$$(1 + xp^\lambda + yp^{\lambda+1})^p \equiv 1 \pmod{p^{\lambda+2}}$$

$$1 + xp^{\lambda+1} \equiv 1 \pmod{p^{\lambda+2}}$$

therefore

$$x = 0,$$

and, therefore,

$$a^{t_\lambda} = 1 + yp^{\lambda+1}$$

$$\equiv 1 \pmod{p^{\lambda+1}}.$$

Therefore

$$t_{\lambda+1} \text{ divides } t_\lambda,$$

which is not so. Therefore we cannot have

$$t_{\lambda+2} = t_{\lambda+1}$$

if

$$t_{\lambda+1} = pt_\lambda,$$

and therefore we must have

$$t_{\lambda+2} = pt_{\lambda+1}.$$

If, then, the exponent of a for modulus p be $t_1 = t$ and $a^t - 1$ contain p^s as the highest power of p, we have

$$a^t \equiv 1 \pmod{p^s},$$

and

$$t_1 = t_2 = \ldots = t_s = t.$$

And after these

$$t_{s+1} = pt_s,$$
$$t_{s+2} = pt_{s+1},$$
$$\&c.$$

Hence the exponent of a for modulus p^λ is

$$t \text{ if } \lambda \leqq s,$$
$$tp^{\lambda - s} \text{ if } \lambda > s,$$

where t is the exponent of a for modulus p, and p^s is the greatest power of p that will divide $a^t - 1$.

Corollary.—The greatest value that t can have is $p - 1$. This is so when a is congruent to a primitive root of p (Proposition 11, corollary). The greatest value that $p^{\lambda - s}$ can have is got by making s as small as possible, viz., by making $s = 1$, *i.e.*, by taking a so that $a^{p-1} - 1$ (though necessarily divisible by p) is not divisible by p^2.

Therefore the greatest possible exponent that a number can have for modulus p^λ is $(p - 1) \,.\, p^{\lambda - 1}$, and as this is equal to $\phi\,(p^\lambda)$ it follows that primitive roots exist for a modulus a power of a prime.

Examples.—Exponent of 3 for mod 5^6.

The exp of 3 for mod 5 is 4 (3. 4. 2. 1).

$3^4 - 1 = 80$ is divisible by 5^1.

Therefore

exp of 3 is $4.\ 5^5 \pmod{5^6}$.

Exponent of 24 for mod 5^6.

The exp of 24 for mod 5 is 2 ($t = 2$).

$24^2 - 1 = 575$ which is divisible by 5^2. ($s = 2$).

Therefore

exp of 24 mod $5^6 = 2.\ 5^4$.

(13.) The exponent to which a number a belongs for a power of 2 as modulus.

The number a is now to be considered odd.

Let $t_1, t_2, t_3, \ldots t_\lambda \ldots$ be the exponents of a for moduli $2, 2^2, \ldots 2^\lambda \ldots$

We have

$$a^{t_{\lambda+1}} \equiv 1 \pmod{2^{\lambda+1}}.$$

Therefore

$$a^{t_{\lambda+1}} \equiv 1 \pmod{2^{\lambda}};$$

therefore

$$t_\lambda \text{ divides } t_{\lambda+1}. \quad \text{(Prop. 2.)}$$

Again

$$a^{t_\lambda} \equiv 1 \pmod{2^\lambda} = 1 + x.2^\lambda + y.2^{\lambda+1} \text{ (where } x = 1 \text{ or } 0).$$

Therefore

$$a^{2t_\lambda} \equiv 1 \pmod{2^{\lambda+1}},$$

and therefore

$$t_{\lambda+1} \text{ divides } 2t_\lambda.$$

Therefore either

$$\left.\begin{array}{l} t_{\lambda+1} = t_\lambda \\ t_{\lambda+1} = 2t_\lambda \end{array}\right\}.$$

or

Suppose now that after

$$t_{\lambda+1} = 2t_\lambda$$

we can have

$$t_{\lambda+2} = t_{\lambda+1}.$$

Then

$$a^{t_\lambda} \equiv 1 \pmod{2^\lambda} = 1 + x.2^\lambda + y.2^{\lambda+1}.$$

Therefore

$$a^{2t_\lambda} \equiv 1 + x.2^{\lambda+1} + x^2 2^{2\lambda} \pmod{2^{\lambda+2}}.$$

Now if $\lambda \overset{=}{>} 2$, then

$$2\lambda \overset{=}{>} \lambda + 2,$$

and therefore

$$a^{2t_\lambda} \equiv 1 + x.2^{\lambda+1} \pmod{2^{\lambda+2}}.$$

Now

$$a^{2t_\lambda} = a^{t_{\lambda+2}} \equiv 1 \pmod{2^{\lambda+2}},$$

therefore

$$x = 0.$$

Therefore

$$a^{t_\lambda} = 1 + x.2^\lambda + y2^{\lambda+1} \equiv 1 \pmod{2^{\lambda+1}},$$

therefore

$$t_{\lambda+1} \text{ divides } t_\lambda,$$

which is not so.

Hence we have the result, when $\lambda \geqq 2$ and $t_{\lambda+1} = 2t_\lambda$, then $t_{\lambda+2} = 2t_{\lambda+1}$.

The first exponent t_1, of the series, is equal to unity.

If this be followed by a set of 1's (at least one), then by what has been proved they will be followed by the series 2, 2^2, 2^3 . . .

If the second exponent be a 2, the third may be also, and so on; the series then continues with $2^2, 2^3, 2^4, \ldots$ Of the 2's there are at least two; for otherwise the first three exponents would be $t_1 = 1$, $t_2 = 2$, $t_3 = 4$, making 4 an exponent for mod $2^3 = 8$, which is impossible.

Hence the series of exponents run either thus—

$$1.\ 1.\ 1.\ \ldots\ 1.\ 2.\ 2^2.\ 2^3.\ 2^4\ \ldots$$

or thus

$$1.\ 2.\ 2.\ \ldots\ 2.\ 2.\ 2^2.\ 2^3.\ 2^4\ \ldots$$

These results can be expressed thus—

Let the highest power of 2 which divides $a^2 - 1$ be 2^{s+1}. (Since a is an odd number, s is at least equal to 2.)

Then the exponent of a is

$$\text{if } \lambda > s,\ 2^{\lambda - s}$$

$$\text{if } \lambda \overset{=}{<} s, \begin{cases} 2 \text{ if } a^2 \equiv 1 \pmod{2^\lambda} \text{ and } a \not\equiv 1 \pmod{2^\lambda}. \\ 1 \text{ if } a \equiv 1 \pmod{2^\lambda}. \end{cases}$$

Corollary.—The greatest exponent possible for mod 2^λ is $2^{\lambda-2}$; and as $\phi(2^\lambda) = 2^{\lambda-1}$, primitive roots do not exist.

Examples.—Exponent of 3 for mod 2^6.

Exp of 3 for mod 2 is 1,
,, ,, 2^2 is 2,
,, ,, 2^3 is 2,
,, ,, 2^4 is 4,

and therefore

exp of 3 for mod 2^6 is 16

Exponent of 35 for mod $64 = 2^6$ ($\lambda = 6$).

$$35^2 - 1 = 1224 = 153.2^3,$$

therefore

$$s = 2,$$

therefore

exp of 35 is 2^4.

Exp of 41 for mod $128 = 2^7$ ($\lambda = 7$).

$$41^2 - 1 = 1680 = 105.2^4,$$

therefore

$$s = 3,$$

therefore

$$\text{exp of } 41 = 2^{7-3} = 2^4.$$

(14.) The numbers which belong to exponent 2 for modulus 2^κ ($\kappa \geqq 3$).

Let a have exponent 2, modulus 2^κ.

Then

$$a^2 \equiv 1 \pmod{2^\kappa}$$

and

$$a \not\equiv 1 \pmod{2^\kappa}.$$

The congruence

$$a^2 \equiv 1 \pmod{2^\kappa}$$

gives

$$(a - 1)(a + 1) \equiv 0 \pmod{2^\kappa}.$$

Since a is odd, if 2^s is the highest power of 2 that divides $a - 1$ and $s > 1$, then the highest power of 2 that divides $a + 1$ is 2, and *vice versâ*.

Hence either

$$a + 1 \equiv 0 \pmod{2^{\kappa-1}},$$

or

$$a - 1 \equiv 0 \pmod{2^{\kappa-1}}.$$

Therefore (excluding $a \equiv 1$ (modulus 2^κ)) we have three numbers whose exponents are 2 for modulus 2^κ, viz.,

$$2^{\kappa-1} + 1, \quad 2^\kappa - 1, \quad 2^{\kappa-1} - 1. \quad \pmod{2^\kappa}.$$

The product of each pair of these is congruent to the third.

$$\left.\begin{array}{l} (2^{\kappa-1} + 1)(2^\kappa - 1) \equiv 2^{\kappa-1} - 1 \\ (2^\kappa - 1)(2^{\kappa-1} - 1) \equiv -2^{\kappa-1} + 1 \equiv 2^{\kappa-1} + 1 \\ (2^{\kappa-1} - 1)(2^{\kappa-1} + 1) \equiv 2^\kappa - 1 \end{array}\right\} \pmod{2^\kappa}.$$

(15.) The numbers which have exponent 2^s for modulus 2^κ.

We have already seen that $s \ngtr \kappa - 2$, and we have already treated (Prop. 14) of the case when $s = 1$.

Let a have exponent 2^s.

The exponents to which it belongs for successive powers of 2 as moduli are given either by

$$\left.\begin{array}{llllllll} \text{exp} & 1. \ 1. \ 1. \ldots & 1 & 2. & 2^2. & \ldots & 2^s \\ \text{mod} & 2. \ 2^2. \ 2^3. \ldots & 2^{\kappa-s}. & 2^{\kappa-s+1}. & 2^{\kappa-s+2}. & \ldots & 2^\kappa \end{array}\right\},$$

or by

$$\left.\begin{array}{l} \text{Exp } 1.\ 2.\ 2.\ \ldots\ \ 2.\ \ \ 2^2.\ \ldots\ 2^s \\ \text{Mod } 2.\ 2^2.\ 2^3.\ \ldots\ 2^{\kappa-s+1}.\ 2^{\kappa-s}.\ \ldots\ 2^\kappa \end{array}\right\}$$

In either case

$$a^2 \equiv 1 \pmod{2^{\kappa-s+1}}$$
$$a^2 \not\equiv 1 \pmod{2^{\kappa-s+2}},$$

therefore

$$a^2 \equiv 1 + 2^{\kappa-s+1} \pmod{2^{\kappa-s+2}},$$

and therefore

$$a \equiv \pm 1 + 2^{\kappa-s} \pmod{2^{\kappa-s+1}}.$$

Thus the numbers (modulus 2^κ) which have exponent 2^s are the 2^s numbers given by

$$\pm 1 + 2^{\kappa-s} \pmod{2^{\kappa-s+1}}.$$

In particular, the numbers with the greatest exponent $2^{\kappa-2}$ are the $2^{\kappa-2}$ numbers

$$\pm 1 + 2^2 \pmod{2^3}.$$

We have seen that there is one number (viz., unity) with exponent 1.

$$\begin{array}{llllll} \text{there are} & 3 & \text{numbers with exponent} & & & 2. \\ ,, \quad ,, & 2^2 & ,, & ,, & ,, & 2^2. \\ & \vdots & & & & \\ ,, \quad ,, & 2^{\kappa-2} & ,, & ,, & ,, & 2^{\kappa-2}. \end{array}$$

In all, $1 + 3 + 2^2 + 2^3 + \ldots + 2^{\kappa-2} = 2^{\kappa-1} = \phi(2^\kappa)$, the number of odd numbers less than 2^κ, as it should be.

(16.) If we take any number g which has exponent $2^{\kappa-2}$ for modulus 2^κ, the successive powers of g give $2^{\kappa-2}$ incongruent numbers, one half of the complete set of odd numbers less than 2^κ.

Of these, one and only one, has exponent 2, viz., $g^{2^{\kappa-3}}$ (Prop. 4).

Now

$$g \equiv \pm 1 + 2^2 \pmod{2^3}$$

squaring,

$$g^2 \equiv 1 + 2^3 \pmod{2^4}$$

and successively squaring

$$g^{2^2} \equiv 1 + 2^4 \pmod{2^5}$$
$$\vdots$$
$$g^{2^{\kappa-3}} \equiv 1 + 2^{\kappa-1} \pmod{2^\kappa}.$$

So of the three numbers $2^\kappa - 1$, $2^{\kappa-1} + 1$, $2^{\kappa-1} - 1$, it is always $2^{\kappa-1} + 1$ to which the power $2^{\kappa-3}$ of any number with exponent $2^{\kappa-2}$ is congruent.

Let f be either of the two numbers $2^\kappa - 1$, $2^{\kappa-1} - 1$; so that $g^{2^{\kappa-3}} \not\equiv f \pmod{2^\kappa}$.

Consider the $2^{\kappa-1}$ numbers

$$\left.\begin{array}{l} g\,,\, g^2\,,\, g^3 \;\ldots\; g^{2^{\kappa-2}} \\ fg, fg^2, fg^3 \ldots\; fg^{2^{\kappa-2}} \end{array}\right\} \pmod{2^\kappa}.$$

Clearly no two in the first row are congruent, nor in the second.

The supposition

$$fg^r \equiv g^{r+t} \pmod{2^\kappa}$$

leads to

$$g^r(g^t - f) \equiv 0 \pmod{2^\kappa}$$
$$g^t \equiv f \pmod{2^\kappa},$$

which is contrary to the supposition that $g^{2^{\kappa-3}}$, and therefore *no* power of g is congruent to f.

Therefore no two of the above $2^{\kappa-1}$ odd numbers are congruent mod 2^κ, and hence they are the $2^{\kappa-1}$ numbers (mod 2^κ).

If for f we take $2^\kappa - 1 \equiv -1 \pmod{2^\kappa}$, the $2^{\kappa-1}$ numbers may be written

$$\pm g,\ \pm g^2,\ \pm g^3, \ldots \pm g^{2^{\kappa-2}} \pmod{2^\kappa}.$$

Whichever number be taken for f, any number (mod 2^κ) is expressible in the form

$$a \equiv f^i g^j \pmod{2^\kappa},$$

where

$$\left.\begin{array}{l} i \text{ is referred to mod } 2, \\ j \text{ is referred to mod } 2^{\kappa-2}. \end{array}\right\}$$

Note.—In the last propositions relating to mod 2^κ, κ is supposed to be $\geqq 3$.

In the case $\kappa = 2$, when the modulus is $2^2 = 4$, there are two odd numbers, less than the modulus, viz., 1 and 3, and 3 (having exponent 2) is a primitive root.

In the case $\kappa = 1$ when the modulus is 2, the only odd number is unity.

We see that the case when the modulus is a power of 2, differs very much from the case when the modulus is a power of an odd prime.

When the mod is 2^κ ($\kappa \geqq 3$).

(i.) The highest exponent is not $\phi(2^\kappa) = 2^{\kappa-1}$, but $2^{\kappa-2}$, and hence there are no primitive roots.

(ii.) The form of the numbers which belong to any exponent is known, and the numbers can be at once written down when κ is known. In particular the numbers $\pm 1 + 2^2$ (mod 8) always belong to the highest exponent.

When the modulus is a power of an odd prime.

(i.) Primitive roots always exist.

(ii.) The determination of primitive roots depends on a knowledge of those of the prime in question.

Examples.—For modulus $2^5 = 32$ the numbers which belong to the different exponents are

Exp 1. 1.
Exp 2. 15. 17. 31.
Exp 4. 7. 23. 9. 25. . . . . ($\pm 1 + 8 \pmod{16}$).
Exp 8. 3. 11. 19. 27. 5. 13. 21. 29 ($\pm 1 + 4 \pmod{8}$).

The residues of powers of 3 are

3. 9. 27. 17. 19. 25. 11. 1.

Multiplying each by $2^5 - 1 = 31$ we get

29. 23. 5. 15. 13. 7. 21. 31,

and, multiplying by $2^4 - 1 = 15$, we get

13. 7. 21. 31. 29. 23. 5. 15,

the same set.

THE Table of Indices for Generators 3 and 15 is—

..	0	1	2	3	4	5	6	7
0	1	3	9	27	17	19	25	11
1	15	13	7	21	31	29	23	5

(Index of 3.)

(Index of 15.)

(17). From propositions (9), (12) and (13) the exponent to which any number a belongs for modulus $m = 2^\kappa p^\lambda q^\mu \ldots$ is readily determined.

For by (9) the exponent is the L.C.M. of the separate exponents of a for moduli 2^κ, p^λ, q^μ, . . . separately.

These exponents are separately determined by propositions (12) and (13).

The greatest possible separate exponents are

$$\left.\begin{array}{ll} 2^{\kappa-2} & \text{if } \kappa \geqq 3 \\ 2 & \text{if } \kappa = 2 \\ 1 & \text{if } \kappa = 1 \end{array}\right\} \text{for mod } 2^\kappa,\ (p-1)\,p^{\lambda-1} \text{ for mod } p^\lambda, \text{ \&c.,}$$

and, hence, the greatest exponent possible for modulus m is the L.C.M. of these.

The value of

$$\phi(m) \text{ is } 2^{\kappa-1}(p-1)\,p^{\lambda-1}(q-1)\,q^{\mu-1}\ldots$$

and, since $p-1$, $q-1$, . . . are all even, the L.C.M. can only equal $\phi(m)$ when

(i.) there is the only one odd prime p present; and
(ii.) $\kappa = 1$ or 0.

Hence the only moduli which admit of primitive roots (which exist only when the highest exponent is equal to $\phi(m)$), are powers of odd primes, and double the powers of odd primes.

Examples.—What is the exponent of 3 for mod $1000000 = 2^6 . 5^6$?

The exp of 3 for mod 2^6 is 2^4.
,, ,, 5^6 is $4 . 5^5$.

Therefore

$$\text{exp of } 3 \text{ mod } 10^6 = 2^4 . 5^5 = 50000.$$

How many decimal places are there in the period of the product of $\cdot\dot{0}\dot{1}$ and $\cdot\dot{0}\dot{1}$, *i.e.*, what is the exponent of 10 for mod $99 \times 99 = 3^4 . 11^2$?

Exp of 10 for mod $3 = 1$.
,, ,, $3^2 = 1$.
,, ,, $3^3 = 3$.
,, ,, $3^4 = 9$.
,, ,, $11 = 2$.
,, ,, $11^2 = 22$.

Therefore

$$\text{exp of } 10 \text{ for mod } 3^4 . 11^2 = 9 \times 22 = 198.$$

Hence there are 198 figures in the period of $(\cdot\dot{0}\dot{1})^2$.

How many decimals are there in the period of $(\cdot\dot{0}0\dot{1})^n$, *i.e.*, what is the exponent of 10 for mod $(999)^n = 37^n . 3^{3n}$?

The exp of 10 mod 3 is 1,

and

$$10 - 1 \text{ is divisible by } 3^2,$$

therefore

$$\text{exp of } 10 \text{ mod } 3^{3n} \text{ is } 3^{3n-2}.$$

$$\text{Exp of } 10 \bmod 37 = 3,$$

and

$$37^1 \text{ divides } 10^3 - 1,$$

therefore

$$\text{exp of } 10 \bmod 37^n = 3 \,.\, 37^{n-1},$$

therefore

$$\text{exp of } 10 \bmod 37^n \,.\, 3^{3n} = 3^{3n-2} \,.\, 37^{n-1},$$

the number of figures in the period.

(18.) We will next briefly consider the residues of successive powers of a number not prime to the modulus.

Let a be the number, m the modulus.

Let $m = p\mathrm{P}$: where p consists of powers of those primes which occur as factors of a, and P is prime to a.

Consider the series of residues

$$a \,.\, a^2 \,.\, a^3 \ldots (\bmod\ m).$$

Suppose that the first term which is repeated is a^r and suppose that

$$a^{r+t} \equiv a^r (\bmod\ m),$$

for which we seek the smallest values of r and t.

Then after the first $r - 1$ terms we shall have a period of t terms constantly repeated.

We have

$$a^r (a^t - 1) \equiv 0 \;(\bmod\ \mathrm{P}p),$$

and P is prime to a. Therefore

$$a^t - 1 \equiv 0 \;(\bmod\ \mathrm{P}) \quad . \; . \; . \; . \; . \; . \; . \; . \; . \; . \quad \text{(i.)}.$$

Each prime factor of p is a factor of a, therefore $a^t - 1$ is prime to p. Therefore

$$a^r \equiv 0 \;(\bmod\ p) \quad . \; . \; . \; . \; . \; . \; . \; . \; . \; . \; . \quad \text{(ii.)}.$$

(i.) Shows that t is the exponent of a for modulus P.

(ii.) Shows that r is the least number that makes a^r divisible by p.

Corollaries.—(i.) When $a \equiv 1$ (mod P) $t = 1$ and the period consists of one term only. (ii.) When a is divisible by p the period starts from the first term. (iii.) When both these hold good, then every power of a is $\equiv a$ (mod m).

Examples.—Residues of powers of 2 mod 100.

$$100 = 5^2 \,.\, 2^2.$$

$$\text{Exp of } 2 \bmod 5 = 4$$

$$\text{,,} \quad \text{,,} \quad 5^2 = 20$$

therefore

$$t = 20,$$

and

$$2^2 \text{ is divided by } 2^2$$

therefore

$$r = 2.$$

$$2.\ \dot{4}.\ 8.\ 16.\ 32.\ 64.\ 28.\ 56.\ 12.\ 24.\ 48.\ 96.\ 92.\ 84.\ 68.\ 36.\ 72.\ 44.\ 88.\ 76.\ \dot{52},$$

the points indicating the period.

Powers of 5 mod $1000 = 2^3 \,.\, 5^3$.

$$5 \text{ has exp } 2 \bmod 2^3,$$

therefore

$$t = 2,$$

$$5^3 \text{ is divided by } 5^3,$$

therefore

$$r = 3.$$

$$5.\ 25.\ \dot{125}.\ \dot{625}.$$

Powers of 5 mod $1000000 = 2^6 \,.\, 5^6$.

$$5 \text{ has exp } 2^4 = 16 \bmod 2^6,$$

therefore

$$t = 16,$$

and

$$5^6 \text{ is divisible by } 5^6,$$

therefore

$$r = 6.$$

$$5.\ 25.\ 125.\ 625.\ 3125.\quad \left.\begin{array}{r} 15625 \\ 78125 \\ 390625 \\ 953125 \\ 765625 \\ 828125 \\ 140625 \\ 703125 \\ 515625 \\ 578125 \\ 890625 \\ 453125 \\ 265625 \\ 328125 \\ 640625 \\ 203125 \end{array}\right\}$$

$$\overline{15625}$$

Powers of $57 \,.\, 5^6 = 890625$ mod 1000000.

$$\text{Exp of } 57 \,.\, 5^6 \bmod 2^6 \text{ is } 1 \; (890625 \equiv 1 \pmod{2^6}),$$

and

$$57 \,.\, 5^6 \text{ is divisible by } 5^6,$$

therefore

$$t = 1$$

and

$$r = 1,$$

and so all powers of 890625 are $\equiv 890625 \pmod{1000000}$.

$$\begin{array}{l} 890625 \\ 890625 \\ \hline 453125 \\ 81250 \\ 3750 \\ 25 \\ \hline 890625 \end{array}$$

(19.) Let $m = p_1 p_2 p_3 \ldots$, where $p_1, p_2, p_3, \ldots$ are co-prime.

Take any number a prime to m.

Suppose that

$$\begin{aligned} a &\equiv \alpha_1 \pmod{p_1}, \\ &\equiv \alpha_2 \pmod{p_2}, \\ &\equiv \alpha_3 \pmod{p_3}, \\ &\quad \&c. \end{aligned}$$

Since a is prime to m and therefore to p_1, it follows that α_1 is prime to p_1. So α_2 is prime to p_2, α_3 to p_3, &c.

Suppose now that, conversely, $\alpha_1, \alpha_2, \alpha_3, \ldots$ prime to $p_1, p_2, p_3, \ldots$ are given, and we wish to find a, such that it is congruent to $\alpha_1 \pmod{p_1}$, $\alpha_2 \pmod{p_2}$, &c.

Let x_1 be determined from

$$x_1 p_2 p_3 \ldots \equiv 1 \pmod{p_1},$$

which can be done, and in one way only, since $p_2 p_3 \ldots$ is prime to p_1; and when x_1 is found let $x_1 p_2 p_3 \ldots \equiv \xi_1$. Determine similarly $\xi_2, \xi_3 \ldots$ Then the number a is given by

$$a \equiv \alpha_1 \xi_1 + \alpha_2 \xi_2 + \alpha_3 \xi_3 + \ldots \pmod{m}.$$

For

$$\xi_2,\ \xi_3,\ \ldots \text{ are all congruent to zero mod } p_1,$$

and

$$\xi_1 \text{ is congruent to unity mod } p_1.$$

Therefore

$$a \equiv \alpha_1 \pmod{p_1},$$

and similarly

$$\equiv \alpha_2 \pmod{p_2},$$

&c.,

and therefore

$$a \equiv \alpha_1\xi_1 + \alpha_2\xi_2 + \alpha_3\xi_3 + \ldots \pmod{m},$$

a formula which gives the value of a corresponding to given values of the α's, the coefficients ξ being independent of the α's and depending only on the moduli $p_1, p_2 \ldots$

Note.—The principal use to be made of this proposition and the next will be for the special case when $p_1, p_2, \ldots$ are the powers of primes of which the modulus m is the product.

(20.) Let us take two numbers expressed in this form,

$$\begin{aligned} a &\equiv \alpha_1\xi_1 + \alpha_2\xi_2 + \ldots \pmod{m}, \\ b &\equiv \beta_1\xi_1 + \beta_2\xi_2 + \ldots \pmod{m}, \end{aligned}$$

in which

$$\left.\begin{aligned} \xi_1 &\equiv 1 \pmod{p_1} \\ &\equiv 0 \left(\text{mod } \frac{m}{p_1}\right) \end{aligned}\right\}$$

with similar relations for $\xi_2, \xi_3, \ldots$

Let us form the product of a and b.

By Proposition (18), Corollary (iii.), all powers of ξ_1 are congruent to ξ_1, mod m, therefore

$$\alpha_1\beta_1\xi_1^2 \equiv \alpha_1\beta_1\xi_1 \pmod{m}.$$

Taking any cross-term such as $\alpha_1\beta_2\xi_1\xi_2$, since

$$\begin{aligned} \xi_1 &\equiv 0 \pmod{p_2 p_3 \ldots}, \\ \xi_2 &\equiv 0 \pmod{p_1 p_3 \ldots}, \end{aligned}$$

therefore

$$\xi_1\xi_2 \equiv 0 \pmod{m}.$$

Hence

$$ab \equiv \alpha_1\beta_1\xi_1 + \alpha_2\beta_2\xi_2 + \alpha_3\beta_3\xi_3 + \ldots \pmod{m},$$

i.e., the multiplication of numbers expressed thus is simply effected by forming the products of the coefficients of $\xi_1, \xi_2 \ldots$

Corollary (i.). If

$$a \equiv \alpha_1\xi_1 + \alpha_2\xi_2 + \ldots + \pmod{m},$$

then

$$a^s \equiv \alpha_1{}^s\xi_1 + \alpha_2{}^s\xi_2 + \ldots \pmod{m}.$$

Corollary (ii.). If

$$a \equiv \alpha_1\xi_1 + \alpha_2\xi_2 + \ldots \pmod{m},$$

then a is congruent to the product of the numbers

$$\begin{cases} a_1 \equiv \alpha_1\xi_1 + \xi_2 + \ldots \pmod{m}, \\ a_2 \equiv \xi_1 + \alpha_2\xi_2 + \ldots \pmod{m}, \\ \text{\&c.} \end{cases}$$

Or, since $\xi_1 + \xi_2 + \ldots \equiv 1 \pmod{m}$ (*cf.* Prop. 10),

$$\begin{cases} a_1 \equiv (\alpha_1 - 1)\,\xi_1 + 1 \pmod{m}, \\ a_2 \equiv (\alpha_2 - 1)\,\xi_2 + 1 \pmod{m}, \\ \ldots\ldots\ldots\ldots \end{cases}$$

Examples.—To find a, modulus 308, so that

$$\begin{aligned} a &\equiv \alpha_1 \pmod{4} \\ &\equiv \alpha_2 \pmod{7} \\ &\equiv \alpha_3 \pmod{11} \end{aligned}$$

$$\begin{array}{rrr} 7.\ 11.\ x_1 \equiv 1 \pmod{4} & 4.\ 11.\ x_2 \equiv 1 \pmod{7} & 4.\ 7.\ x_3 \equiv 1 \pmod{11} \\ 3.\quad 3.\ x_1 \equiv 1 \pmod{4} & 2.\ x_2 \equiv 1 \pmod{7} & 6.\ x_3 \equiv 1 \pmod{11} \\ x_1 \equiv 1 \pmod{4} & x_2 \equiv 4 \pmod{7} & x_3 \equiv 2 \pmod{11} \\ \xi_1 \equiv 77 \pmod{308} & \xi_2 \equiv 176 \pmod{308} & \xi_3 \equiv 56 \pmod{308} \end{array}$$

and so

$$a \equiv 77\,\alpha_1 + 176\,\alpha_2 + 56\,\alpha_3 \pmod{308},$$

e.g.,

$$\begin{aligned} a &\equiv 3 \pmod{4} \\ &\equiv 6 \pmod{7} \\ &\equiv 1 \pmod{11} \end{aligned}$$

then

$$\begin{aligned} a &\equiv 77.\,3 + 176.\,6 + 56.\,1 \pmod{308} \\ &\equiv 111\ (\text{mod. } 308), \end{aligned}$$

and

$$\begin{aligned} 111 &\equiv (77.\,3 + 176 + 56)\,(77 + 176.\,6 + 56)\,(77 + 176 + 56) \\ &\equiv 155.\,265 \pmod{308}. \end{aligned}$$

(21.) The number of numbers which belong to a given exponent when the modulus is a power of a prime.

I. Let the prime be an odd prime, and p^λ the modulus.

In Proposition (12), Corollary, we saw that for mod p^λ primitive roots exist.

Let g be a primitive root.

The numbers $g, g^2, g^3, \ldots g^{\phi(p^\lambda)} \pmod{p^\lambda}$ are congruent to the complete set of numbers less than p^λ and prime to it.

The exponent to which any one of these numbers, g^s, belongs is t, where

and $$\left.\begin{aligned} \phi(p^\lambda) &= \kappa t \\ s &= \kappa\sigma \end{aligned}\right\} \text{ and } t \text{ and } \sigma \text{ are co-prime (Prop. 4).}$$

For any given value of t the value of $\kappa = \phi(p^\lambda)/t$ is given.

σ may then have any value prime to t such that

$$s \ngtr \phi(p^\lambda),$$

i.e.,

$$\kappa\sigma \ngtr \kappa t$$

$$\sigma \ngtr t.$$

Hence σ may have each of the $\phi(t)$ values of the numbers less than t and prime to it.

Therefore there are $\phi(t)$ numbers having t as their exponent (mod m).

II. Let the modulus be 2^κ. ($\kappa \geqq 3$).

In this case we have seen (Proposition 15) that there are 2^s numbers with exponent 2^s (if $s > 1$): and 3 numbers with exponent 2; and 1 number with exponent unity.

When the modulus is 2^2 there is one number with exponent 2 and one with unity.

When the modulus is 2 there is one number (unity) with exponent unity.

Definition.—When a number m is expressed in the form $m = 2^\kappa P_1^{\lambda_1} P_2^{\lambda_2} \ldots$ where $P_1, P_2, \ldots$ are different odd primes, it will be convenient to speak of $2^\kappa, P_1^{\lambda_1}, P_2^{\lambda_2} \ldots$ as the *principal factors* of m.

(22.) The number of numbers, each of which has, as exponent, some power of a prime p, for modulus m, p being a divisor of $\phi(m)$.

Let

$$m = 2^\kappa P_1^{\lambda_1} P_2^{\lambda_2}, \ldots$$

$$\phi(P_1^{\lambda_1}) = 2^{\kappa_1} p^{l_1} q^{m_1}, \ldots$$

$$\phi(P_2^{\lambda_2}) = 2^{\kappa_2} p^{l_2} q^{m_2}, \ldots$$

&c.

Any number has for its exponent, modulus m, the L.C.M. of its separate exponents for moduli 2^κ, $P_1^{\lambda_1}$, $P_2^{\lambda_2}$, . . . the principal factors of m. (Proposition (9), Corollary.)

Hence, when the exponent, modulus m, is a power of a prime p, the exponent for each of the principal factors of m as moduli, must each be either unity or some power of p.

Conversely, if we take a set of numbers $\alpha_0, \alpha_1, \alpha_2, \ldots$ one for each of the moduli 2^κ, $P_1^{\lambda_1}, \ldots$ such that the exponent of each, for its own modulus, is unity or some power of p, then the number $a \equiv \alpha_0\xi_0 + \alpha_1\xi_1 + \ldots \pmod{m}$, will have a power of p as exponent, modulus m.

The numbers ξ are given by

$$\begin{array}{ll} \xi_0 \equiv 1 \ (\text{mod } 2^\kappa), & \xi_1 \equiv 1 \ (\text{mod } P_1^{\lambda_1}), \\ \equiv 0 \left(\text{mod } \dfrac{m}{2^\kappa}\right), & \equiv 0 \left(\text{mod } \dfrac{m}{P^{\lambda_1}}\right), \end{array} \quad \&\text{c.}$$

Thus, by giving to the α's all possible sets of values consistently with each having unity or a power of p as exponent, we shall obtain all the numbers (mod m) which have (unity or) a power of p as exponent.

There are

$$\left\{\begin{array}{lllll} \phi\,(p^{l_1}) & \text{numbers which} & \text{have} & \text{exp } p^{l_1}, & \text{mod } P_1^{\lambda_1}. \quad (\text{Prop. } 21.) \\ \phi\,(p^{l_1-1}) & \quad ,, & \ ,, & \quad ,, \ p^{l_1-1} & \quad ,, \\ \quad \&\text{c.} & & & & \\ \quad 1 & \quad ,, & \ ,, & \quad ,, \ \ 1 & \quad ,, \end{array}\right.$$

Hence there are $\phi\,(p^{l_1}) + \phi\,(p^{l_1-1}) + \ldots + 1 = p^{l_1}$ numbers, mod $P_1^{\lambda_1}$, which have unity or a power of p as exponent.

Similarly, there are p^{l_2} for mod $P_2^{\lambda_2}$, and so on.

Hence, in

$$a \equiv \alpha_0\xi_0 + \alpha_1\xi_1 + \alpha_2\xi_2 + \ldots \pmod{m},$$

$$\left.\begin{array}{l} \text{we can give 1 value (viz., unity) to } \alpha_0 \\ \text{any one of } p^{l_1} \text{ values to } \alpha_1 \\ \quad ,, \qquad p^{l_2} \qquad ,, \qquad \alpha_2 \\ \qquad \&\text{c.,} \qquad\qquad \&\text{c.} \end{array}\right\}$$

and then a has unity or a power of p as exponent, mod m; moreover, in this way, all such numbers are obtained.

We thus obtain $p^{l_1+l_2+\cdots} = p^{\Sigma l}$ incongruent numbers, each of which has a power of p (or unity) for exponent.

In the case when $p = 2$

for mod 2^κ, all $2^{\kappa-1}$ numbers have powers of 2 as exponents,
,, $P_1^{\lambda_1}$, $\phi(2^{\kappa_1}) + \phi(2^{\kappa_1-1}) + \ldots + 1 = 2^{\kappa_1}$ have powers of 2 as exponents,
,, $P_2^{\lambda_2}$, $\phi(2^{\kappa_2}) + \phi(2^{\kappa_2-1}) + \ldots + 1 = 2^{\kappa_2}$,, ,, ,,
&c. &c. &c.

Hence, in all, there are $2^{\kappa-1+\kappa_1+\kappa_2+\ldots}$ numbers, which have unity or a power of 2 as exponent.

Note.—Any number a, mod m, with any exponent, must be congruent to a product of one number from each set of $2^{\kappa-1+\kappa_1+\kappa_2+\ldots}$ numbers, with powers of 2 as exponent, $p^{\Sigma l}$ with powers of p as exponent, . . . &c. (Proposition 10.)

Hence in all we get from these

$$\begin{aligned} &2^{\kappa-1+\kappa_1+\ldots}\, p^{\Sigma l} q^{\Sigma m} \ldots \text{ numbers,} \\ &= \phi(2^\kappa)\, \phi(P_1^{\lambda_1}) \ldots \quad ,, \\ &= \phi(m) \text{ numbers, } i.e., \text{ the complete set of numbers prime to } m. \end{aligned}$$

(23.) The number of numbers having exponent p^s, mod m, p^s being a divisor of the greatest exponent.

Let a be such a number and let

$$a \equiv \alpha_0\xi_0 + \alpha_1\xi_1 + \alpha_2\xi_2 + \ldots \pmod{m},$$

then the exponent of

$$\left.\begin{array}{l} \alpha_0 \bmod 2^\kappa \\ \alpha_1 \bmod P_1^{\lambda_1} \\ \alpha_2 \bmod P_2^{\lambda_2} \\ \quad \&c. \end{array}\right\}$$

must each be unity or some power of p, and the greatest power of p must be p (Proposition (9), Corollary); p being an odd prime α_0 is necessarily unity.

There are

$\phi(p^{l_1})$ numbers, mod $P_1^{\lambda_1}$ with exp p^{l_1},
$\phi(p^{l_1-1})$,, ,, ,, ,, p^{l_1-1},
&c., &c.,

and therefore there are

p^{l_1} numbers with exp a power of $p \leqq p^{l_1}$,
p^{l_1-1} ,, ,, ,, ,, $\leqq p^{l_1-1}$,
&c., &c.

Hence if

$$\left.\begin{array}{ll} & l_1 < s \text{ there are } p^{l_1} \text{ numbers, mod } \mathrm{P}_1^{\lambda_1}, \text{ with exp a power of } p \ngtr p^s \\ \text{and if} & \\ & l_1 \geqq s \text{ there are } p^{s} \text{ numbers, mod } \mathrm{P}_1^{\lambda_1}, \text{ with exp a power of } p \ngtr p^s \end{array}\right\}$$

Suppose that $(l_1)_s$ stands for s if $l_1 \geqq s$ and for l_1 if $l_1 < s$, then in either case there are $p^{(l_1)_s}$ numbers, mod $\mathrm{P}_1^{\lambda_1}$, whose exponents are powers of $p \ngtr p^s$.

Similarly there are $p^{(l_2)_s}$ numbers mod $\mathrm{P}_2^{\lambda_2}$, whose exponents are powers of $p \ngtr p^s$ and so for $\mathrm{P}_2^{\lambda_2}$, &c.

Giving any one of these $p^{(l_1)_s}$ values to α_1, $p^{(l_2)_s}$ values to α_2, &c., we obtain

$$p^{(l_1)_s + (l_2)_s + \ldots} = p^{(\Sigma l)_s} \text{ numbers, mod } m,$$

whose exponents are powers of $p \ngtr p^s$; where in $p^{(\Sigma l)_s}$ each number l in $l_1 + l_2 + \ldots$ is to be replaced by s if it exceeds s.

Similarly, there are $p^{(\Sigma l)_{s-1}}$ numbers, mod m, whose exponents are powers of $p \ngtr p^{s-1}$ &c., &c., $p^{(\Sigma l)_1}$ numbers with exponents p or unity, and 1 number with exponent 1.

Hence the number of numbers whose exponent is p^s, mod m, is

$$p^{(\Sigma l)_s} - p^{(\Sigma l)_{s-1}}, \text{ which when } s = 1 \text{ is } p^{(\Sigma l)_1} - 1.$$

Corollary.—If p^s be the highest power of p which can be an exponent for mod m, *i.e.*, if p^s is the highest power of p that divides the greatest exponent, *i.e.*, if s is the greatest of the numbers $l_1, l_2, \ldots$ then

$$1 + (p^{(\Sigma l)_1} - 1) + (p^{(\Sigma l)_2} - p^{(\Sigma l)_1}) + \ldots + (p^{(\Sigma l)_s} - p^{(\Sigma l)_{s-1}}) = p^{(\Sigma l)_s}$$

is the number of numbers having as exponent (mod m) a power of p (or unity) as exponent.

Now since s is equal to the greatest of the quantities $l_1, l_2, \ldots$ (or rather is not less than any) $(\Sigma l)_s = \Sigma l$ and therefore $p^{(\Sigma l)_s} = p^{\Sigma l}$: the result which was obtained in the last proposition.

(23A.) To find the number of numbers having exponent 2^σ, mod m.

(It will be convenient to write now $\kappa = \kappa' + 2$, so that $m = 2^{\kappa'+2}\mathrm{P}_1^{\lambda_1}\mathrm{P}_2^{\lambda_2}\ldots$).

If a be any such number, and

$$a \equiv \alpha_0\xi_0 + \alpha_1\xi_1 + \ldots (\text{mod } m),$$

the exponents of

$$\left.\begin{array}{c} \alpha_0 \text{ mod } 2^\kappa \\ \alpha_1 \text{ mod } \mathrm{P}_1^{\lambda_1} \\ \alpha_2 \text{ mod } \mathrm{P}_2^{\lambda_2} \\ \text{\&c.} \end{array}\right\}$$

must each be unity or a power of 2, and the greatest power of 2 must be 2^σ.

First suppose that $\kappa \geqq 3$, and so $\kappa' \geqq 1$.

Then there are, mod $2^{\kappa'+2}$,

$$\left.\begin{array}{llllll}
2^{\kappa'} & \text{numbers} & \text{with} & \text{exponent} & 2^{\kappa'} \\
2^{\kappa'-1} & ,, & ,, & ,, & 2^{\kappa'-1} \\
\vdots & & & & \\
2^{2} & ,, & ,, & ,, & 2^{2} \\
3 & ,, & ,, & ,, & 2 \\
1 & \text{number} & ,, & ,, & 1
\end{array}\right\}$$

Hence there are

$$\begin{array}{llllll}
2^{\kappa'+1} & \text{numbers with exponent a power of 2} & & & & \ngtr 2^{\kappa'} \\
2^{\kappa'} & ,, & ,, & ,, & ,, & \ngtr 2^{\kappa'-1} \\
\vdots & & & & & \\
2^{2} & ,, & ,, & ,, & ,, & \ngtr 2 \\
1 & \text{number} & ,, & ,, & ,, & \ngtr 2^{0}
\end{array}$$

If

$\sigma > \kappa'$ then there are $2^{\kappa'+1}$ numbers with exponent a power of $2 \ngtr 2^{\sigma}$, mod $2^{\kappa'+2}$,

and if

$\sigma \leqq \kappa'$ then ,, ,, $2^{\sigma+1}$,, ,, ,, ,, ,, ,,

(this holds unless $\sigma = 0$, and then there is one number (unity) with exponent 1).

In either case, then, there are $2^{(\kappa')_{\sigma}+1}$ numbers with powers of $2 \ngtr 2^{\sigma}$ as exponents, where $(\kappa')_{\sigma}$ is to be replaced by

$$\left.\begin{array}{l}
\sigma \text{ if } \kappa' > \sigma \\
\kappa' \;,,\; \kappa' \leqq \sigma
\end{array}\right\}.$$

Next for mod $P_1^{\lambda_1}$ there are

$$\begin{array}{llllll}
2^{\kappa_1-1} & \text{numbers with exponent a power of 2} & & & & \ngtr 2^{\kappa_1-1} \\
2^{\kappa_1-2} & ,, & ,, & ,, & ,, & \ngtr 2^{\kappa_1-2} \\
\text{\&c.} & & & & &
\end{array}$$

Hence (using the same notation) there are $2^{(\kappa_1)_{\sigma}}$ numbers (mod $P_1^{\lambda_1}$) having exponent a power of $2 \ngtr 2^{\sigma}$.

Thus α_0 may have each of $2^{(\kappa')_{\sigma}}$ values, α_1 each of $2^{(\kappa_1)_{\sigma}}$ values, &c., and the corresponding value of a has exponent a power of 2 (mod m), $\ngtr 2^{\sigma}$.

Hence the number of these is $2^{(\Sigma\kappa)_{\sigma}+1}$, where in $\Sigma\kappa = \kappa' + \kappa_1 + \kappa_2 + \ldots$ each number κ is to be replaced by σ if it exceeds σ.

Similarly the number of numbers whose exponent, mod m, is a power of $2 \not> 2^{\sigma-1}$ is

$$2^{(\Sigma\kappa)_{\sigma-1}+1}.$$

Hence the number of numbers with exponent 2^σ (mod m) is

$$2^{(\Sigma\kappa)_\sigma+1} - 2^{(\Sigma\kappa)_{\sigma-1}+1}.$$

This holds for $\sigma \overset{=}{>} 2$. When $\sigma = 1$ the number of numbers with exponent 2 is

$$2^{(\Sigma\kappa)_1+1} - 1.$$

Secondly suppose that $\kappa = 2$, and so $\kappa' = 0$.

Then, if σ is > 1, α_0 may be either 1 or 3, two values.

Hence the number of numbers with exponent 2^σ is

$$2^{(\Sigma\kappa)_\sigma+1} - 2^{(\Sigma\kappa)_{\sigma-1}+1},$$

which agrees with the above when κ' is omitted.

If $\sigma = 1$, the number of numbers with exponent 1 or 2, mod 2^2, is 2.

Therefore the number of numbers with exponent 2, mod m, is

$$2^{(\Sigma\kappa)_1+1} - 1,$$

which agrees with the above when κ' is put $= 0$.

Thirdly, let $\kappa = 1$. Then α_0 must be unity and the number of numbers with exponent 2^σ is $2^{(\Sigma\kappa)_\sigma} - 2^{(\Sigma\kappa)_{\sigma-1}}$ where $\Sigma\kappa = \kappa_1 + \kappa_2 + \ldots$

Fourthly, when ($\kappa = 0$) m is odd, then again the number required is $2^{(\Sigma\kappa)_\sigma} - 2^{(\Sigma\kappa)_{\sigma-1}}$.

To collect the results :—

When

$$\left.\begin{array}{rl} m = & 2^{\kappa'+2}P_1^{\lambda_1}P_2^{\lambda_2}\ldots \\ \text{or} & 2^2P_1^{\lambda_1}P_2^{\lambda_2}\ldots \end{array}\right\} \begin{array}{l} \text{there are } 2^{(\Sigma\kappa)_1+1} - 1 \text{ numbers with exp } 2, \\ \qquad 2^{(\Sigma\kappa)_\sigma+1} - 2^{(\Sigma\kappa)_{\sigma-1}+1} \text{ numbers with exp } 2^\sigma. \end{array}$$

And when

$$\left.\begin{array}{rl} m = & 2P_1^{\lambda_1}P_2^{\lambda_2}\ldots \\ \text{or} & P_1^{\lambda_1}P_2^{\lambda_2}\ldots \end{array}\right\} \begin{array}{l} \text{there are } 2^{(\Sigma\kappa)_1} - 1 \text{ numbers with exp } 2, \\ \qquad 2^{(\Sigma\kappa)_\sigma} - 2^{(\Sigma\kappa)_{\sigma-1}} \text{ numbers with exp } 2^\sigma. \end{array}$$

(23B.) The last two propositions give us the number of numbers belonging to any exponent $t = 2^a p^b q^c \ldots$

For the complete set of these numbers is formed by taking all possible products of a number with exponent 2^a, one with exponent p^b, &c.

Hence the number of numbers with exponent t is the product of the number of numbers that belong to each of its principal factors as exponent.

Examples.—The number of numbers that belong to any exponent for mod $m = 2^4 . 13 . 17 . 19$.

The greatest exponent is the L.C.M. of

$$\left.\begin{array}{l} \phi(2^4) = 2^3 \\ \phi(13) = 2^2 . 3 \\ \phi(17) = 2^4 \\ \phi(19) = 2 . 3^2 \end{array}\right\} = 2^4 . 3^2. \qquad \phi(m) = 2^{10} . 3^3.$$

For the 2-power exponent numbers we have for the κ's

$$\kappa' = 2 \qquad \kappa_1 = 2 \qquad \kappa_2 = 4 \qquad \kappa_3 = 1.$$

$$\left.\begin{array}{l} (\Sigma\kappa)_1 = 4 \\ (\Sigma\kappa)_2 = 7 \\ (\Sigma\kappa)_3 = 8 \\ (\Sigma\kappa)_4 = 9 \end{array}\right\}.$$

Therefore

$$\left.\begin{array}{l} \text{belonging to exp } 2^4 \text{ there are } 2^{10} - 2^9 \text{ numbers} \\ \quad ,, \qquad ,, \quad 2^3 \text{ there are } 2^9 - 2^8 \text{ numbers} \\ \quad ,, \qquad ,, \quad 2^2 \text{ there are } 2^8 - 2^5 \text{ numbers} \\ \quad ,, \qquad ,, \quad 2 \text{ there are } 2^5 - 1 \text{ numbers} \end{array}\right\}.$$

For the 3-power exponent numbers we may take $l_1 = 1, \quad l_2 = 2$,

$$(\Sigma l)_1 = 2,$$
$$(\Sigma l)_2 = 3.$$

$$\left.\begin{array}{l} \text{Belonging to exp } 3^2 \text{ there are } 3^3 - 3^2 \text{ numbers} \\ \quad ,, \qquad ,, \quad 3 \text{ there are } 3^2 - 1 \text{ numbers} \end{array}\right\}.$$

The number of numbers belonging to any other exponent is at once got from these by multiplying, *e.g.*, the number of numbers with the greatest exponent $2^4 . 3^2$ is $(2^{10} - 2^9)(3^3 - 3^2)$.

(24.) We shall now establish a particular set of independent generators which generate the $\phi(m)$ numbers (mod m) prime to m.

Any number a, mod m, is expressible in the form

$$a \equiv \alpha_0\xi_0 + \alpha_1\xi_1 + \alpha_2\xi_2 + \ldots \text{ (mod } m).$$

Let

and let

$$\left.\begin{array}{l} g_1 \text{ be a primitive root of } \mathrm{P}_1^{\lambda_1} \\ g_2 \qquad ,, \qquad\qquad ,, \qquad \mathrm{P}_2^{\lambda_2} \\ \qquad \&\text{c.} \qquad\qquad \&\text{c.}, \\ \\ g_0 \text{ have exp } 2^{\kappa-2} \bmod 2^{\kappa} \\ f \text{ be} \equiv 2^{\kappa} - 1 \text{ or } 2^{\kappa-1} - 1 \bmod 2^{\kappa} \end{array}\right\}$$

(In the case when $\kappa = 2$, f does not occur, when $\kappa = 1$ or 0, neither f nor g_0.)

Then

and

$$\left.\begin{array}{l} \alpha_1 \equiv g_1^{i_1} \pmod{\mathrm{P}_1^{\lambda_1}} \\ \alpha_2 \equiv g_2^{i_2} \pmod{\mathrm{P}_2^{\lambda_2}} \\ \qquad \&\text{c.}, \\ \\ \alpha_0 \equiv g_0^{i_0} f^{j} \pmod{2^{\kappa}} \end{array}\right\} \text{say.}$$

Therefore

$$\begin{aligned} a &\equiv g_0^{i_0} f^{j} \xi_0 + g_1^{i_1} \xi_1 + \ldots \pmod{m} \\ &\equiv (f\xi_0 + \xi_1 + \ldots)^{j} (g_0\xi_0 + \xi_1 + \ldots)^{i_0} (\xi_0 + g_1\xi_1 + \ldots)^{i_1} \ldots \pmod{m} \\ &\equiv [(f-1)\,\xi_0 + 1]^{j} [(g_0 - 1)\,\xi_0 + 1]^{i_0} [(g_1 - 1)\,\xi_1 + 1]^{i_1} \ldots \pmod{m}, \end{aligned}$$

where

$$\begin{array}{llll} j & \text{is referred to} & \bmod 2, & \\ i_0 & \quad ,, & \quad ,, \quad \bmod 2^{\kappa-2}, & \\ i_1 & \quad ,, & \quad ,, \quad \bmod \phi(\mathrm{P}_1^{\lambda_1}), & \\ & & \&\text{c.}, & \end{array}$$

and so the set of indices j, i_0, $i_1 \ldots$ correspond uniquely to the number a: and the numbers

$$(f-1)\,\xi_0 + 1, \quad (g_0 - 1)\,\xi_0 + 1, \quad (g_1 - 1)\,\xi_1 + 1, \ldots$$

are a set of independent generators, with exponents

$$2, \qquad 2^{\kappa-2}, \qquad \phi(\mathrm{P}_1^{\lambda_1}), \ldots$$

which generate completely the $\phi(m)$ numbers, mod m, which are prime to m.

Example.—Take the modulus

$$m = 112 = 2^4.\,7. \qquad \phi(m) = (2^3)\,(2.\,3) = 2^4.\,3 = 48.$$

If

$$a \equiv \alpha_0 \pmod{2^4},$$

and

$$a \equiv \alpha_1 \ (\text{mod } 7),$$
$$a \equiv \alpha_0 \xi_0 + \alpha_1 \xi_1 \ (\text{mod } 112).$$

$$\begin{array}{ll} 7x_0 \equiv 1 \ (\text{mod } 2^4) & 2^4 x_1 \equiv 1 \ (\text{mod } 7) \\ x_0 \equiv 7 \ (\text{mod } 2^4) & 2x_1 \equiv 1 \ (\text{mod } 7) \\ \xi_0 \equiv 49 \ (\text{mod } 112) & x_1 \equiv 4 \ (\text{mod } 7) \\ & \xi_1 \equiv 64 \ (\text{mod } 112), \end{array}$$

$$a \equiv 49\alpha_0 + 64\alpha_1 \ (\text{mod } 112).$$

We will take

$$f = 7 \ (= 2^3 - 1)$$
$$g_0 = 3 \ (\text{having exp } 2^2),$$

and

$$g_1 = 3 \ (\text{a primitive root of } 7).$$

Then

$$(f - 1)\,\xi_0 + 1 = 6.\,49 + 1 = 295 \equiv 71 \ (\text{mod } 112),$$
$$(g_0 - 1)\,\xi_0 + 1 = 2.\,49 + 1 = 99 \ (\text{mod } 112),$$
$$(g_1 - 1)\,\xi_1 + 1 = 2.\,64 + 1 = 129 \equiv 17 \ (\text{mod } 112);$$

and

$$\left.\begin{array}{l} 71 \text{ with exp } 2 \\ 99 \text{ with exp } 4 \\ 17 \text{ with exp } 6 \end{array}\right\} \text{generate the 48 numbers prime to 112.}$$

The following table gives the indices corresponding to any number :—

Numbers	1.	3.	5.	9.	11.	13.	15.	17.	19.	23.	25.	27.	29.	31.	33.	37.	39.	41.	43.	45.	47.	51.	53.	55.	57.	59.
Ind. of 17	0	1	5	2	4	3	0	1	5	2	4	3	0	1	5	2	4	3	0	1	5	2	4	3	0	1
Ind. of 99	0	1	1	2	3	3	2	0	1	0	2	3	3	2	0	1	0	2	3	3	2	1	1	0	2	3
Ind. of 71	0	0	1	0	0	1	1	0	0	1	0	0	1	1	0	1	1	0	0	1	1	0	1	1	0	0

Numbers	61.	65.	67.	69.	71.	73.	75.	79.	81.	83.	85.	87.	89.	93.	95.	97.	99.	101.	103.	107.	109.	111
Ind. of 17	5	2	4	3	0	1	5	2	4	3	0	1	5	2	4	3	0	1	5	2	4	3
Ind. of 99	3	0	1	1	0	2	3	2	0	1	1	0	2	3	2	0	1	1	0	3	3	2
Ind. of 71	1	0	0	1	1	0	0	1	0	0	1	1	0	1	1	0	0	1	1	0	1	1

We proceed now to the point we have been approaching from the beginning, viz., the investigation of the mode of formation of and the relations among the most general set of numbers capable of generating the $\phi(m)$ numbers (modulus m) which are prime to the modulus m.

(25.) Suppose $G_1, G_2, G_3, \ldots$ with exponents $t_1, t_2, \ldots$ are capable of acting as complete generators of the $\phi(m)$ numbers.

Then

$$\text{(i.) } t_1 t_2 t_3 \ldots = \phi(m)$$

and

(ii.) the generators must be independent.

Since the numbers G generate the complete set of $\phi(m)$ numbers they can generate in particular the numbers which have a power of a prime p (which is a factor of $\phi(m)$) as exponent.

Suppose the highest powers of p which occur in $t_1, t_2, \ldots$ are $p^{s_1}, p^{s_2}, \ldots$ respectively.

Say

$$\left.\begin{array}{c} t_1 = p^{s_1} t'_1, \\ t_2 = p^{s_2} t'_2, \\ \text{\&c.} \end{array}\right\}$$

Then we can express the numbers G thus (Proposition 10) :—

$$\begin{gathered} G_1 \equiv g_1 h_1 \pmod{m}, \\ G_2 \equiv g_2 h_2 \pmod{m}, \\ \text{\&c.}, \end{gathered}$$

when g_1 has exponent p^{s_1} and h_1 has exponent t'_1, &c.

Suppose now that

$G_1^{i_1} G_2^{i_2} G_3^{i_3} \ldots$ is congruent to a number with a power of p as exponent,

and so

$(g_1^{i_1} g_2^{i_2} \ldots)(h_1^{i_1} h_2^{i_2} \ldots)$,, ,, ,, ,, ,,

g_1, and therefore $g_1^{i_1}$, has a power of p as exponent (Proposition 4), and so for $g_2^{i_2}$, &c.

Therefore

$g_1^{i_1} g_2^{i_2} \ldots$ has a power of p as exponent.

The exponent of h_1, and therefore of $h_1^{i_1}$, is prime to p, and so for $h_2^{i_2}, \ldots$ &c.

Therefore the exponent of $h_1^{i_1} h_2^{i_2} \ldots$ which divides the L.C.M. of the exponents of $h_1^{i_1}, h_2^{i_2}, \ldots$ is prime to p.

Therefore the exponent of $(g_1^{i_1} g_2^{i_2} \ldots)(h_1^{i_1} h_2^{i_2} \ldots)$ is the L.C.M. of a power of p and of a number (the exponent of $h_1^{i_1} h_2^{i_2} \ldots$) prime to p. Now the exponent is to be a power of p. Hence the exponent of $h_1^{i_1} h_2^{i_2} \ldots$ must be unity.

Therefore

$$h_1^{i_1} h_2^{i_2} \ldots \equiv 1 \pmod{m}.$$

Now we can show that this cannot be unless

$$h_1^{i_1} \equiv 1,\ h_2^{i_2} \equiv 1, \ldots \pmod{m}.$$

For if not suppose that at least $i_1 \not\equiv 0$ (modulus t'_1).

Then

$$h_1^{i_1} h_2^{i_2} \ldots \equiv h_1^{t'_1} \pmod{m},$$
$$h_2^{i_2} h_3^{i_3} \ldots \equiv h_1^{t'_1 - i_1} \pmod{m}.$$

Let

$I_2 \equiv i_2 \pmod{t'_2}$ and the same for I_3, &c. : and $I_1 \equiv - i_1 \pmod{t'_1}$

$\equiv 0 \pmod{p^{s_2}}$, $\qquad \equiv 0 \pmod{p^{s_1}}$,

so that $I_2 < t_2$ $\qquad$ so that $I_1 < t_1$

and $\left.\begin{array}{l} g_2^{I_2} \equiv 1 \\ h_2^{I_2} \equiv h_2^{i_2} \end{array}\right\} \pmod{m}$ $\qquad$ $\begin{array}{l} g_1^{I_1} \equiv 1 \pmod{m} \\ h_1^{I_1} \equiv h_1^{t'_1 - i_1} \pmod{m}, \end{array}$

then

$$G_2^{I_2} G_3^{I_3} \ldots \equiv G_1^{I_1} \pmod{m},$$

where

$$I_1 \not\equiv 0 \pmod{t_1},$$

which is contrary to the supposition that the generators G are *independent*, and that therefore no two numbers of the $t_1 t_2 \ldots$ that they generate shall be congruent.

Therefore we must have

$$i_1 \equiv 0 \pmod{t'_1},$$
$$i_2 \equiv 0 \pmod{t'_2},$$
&c.

and so

$$h_1^{i_1} \equiv 1 \pmod{m},$$
$$h_2^{i_2} \equiv 1 \pmod{m},$$
&c.

and so

$$G_1^{i_1} \equiv g_1^{i_1} \pmod{m},$$
&c.

We have shown, then, that when a product of powers of the generators G, $G_1^{i_1} G_2^{i_2} \ldots$ is congruent to a number with a power of a prime p as exponent, then each factor, $G_1^{i_1}$, $G_2^{i_2}$, ... must have a power of p for its exponent.

Thus, of the factors of the product to which G_1 is congruent, each factor having a principal factor of t_1 as exponent (Proposition 10), only one factor g_1 (viz., that which has, as exponent, a power of p) is effective in any power of G_1 which can be used to form a number with exponent a power of p, the product of the remaining factors h_1 being necessarily raised to such a power i_1 that $h_1^{i_1} \equiv 1 \pmod{m}$.

(It will be convenient to call the numbers which have a power of p as exponent, the "p-power-exponent numbers").

Suppose then that we take the generators G, and express each as a product in the manner of Proposition 10. Then take from each the factor (if any) which has a power of the prime p as exponent. Then, since the numbers G can generate all the numbers, modulus m, which have a power of p as exponent, and, since in the number G the factor g is alone effective in so doing, it follows that the set of numbers g generate completely the p-power-exponent numbers.

If we take from each generator G the factor which has a power of any other prime q as exponent, we obtain a set of numbers g', which generate the q-power-exponent numbers, and so on for each prime which divides $\phi(m)$.

We see now, that any set of complete independent generators, G, must be formed from these special sets of generators; the formation of each G being effected by taking one number (which may be unity) from each set and forming their product.

In order to obtain the most general set of generators, G, we have now only to obtain the most general method of producing each of these subsidiary sets of generators. We may then combine them as products (one from each set) in any manner we please.

(26.) Suppose that $\Gamma_1, \Gamma_2, \ldots$ independent generators, generate completely the p-power-exponent numbers.

The exponent of each number, Γ, must be some power of p.

Let them be $p^{n_1}, p^{n_2}, \ldots$ respectively.

One condition that the numbers, Γ, must satisfy is that the number of numbers they generate, which belong to any power of p, p^s as exponent, should agree with the number already found. (Proposition 23.)

Consider any number generated

$$a \equiv \Gamma_1^{i_1}\Gamma_2^{i_1} \ldots \pmod{m}.$$

Since $\Gamma_1, \Gamma_2, \ldots$ are *independent* generators, therefore the exponent of a is the greatest of the separate exponents of $\Gamma_1^{i_1}, \Gamma_2^{i_2}, \ldots$ (Proposition 8. Corollary).

Now Γ_1 has exponent p^{n_1}, therefore of the numbers of the form $\Gamma_1^{i_1}$, there are

$$\begin{array}{llll} p^{n_1} \text{ with exponent a power of } p & \ngtr p^{n_1}, \\ p^{n_1-1} \quad ,, \qquad ,, \qquad ,, & \ngtr p^{n_1-1}, \\ \quad \&\text{c.}, & \end{array}$$

and similarly for each of the others, $\Gamma_2, \Gamma_3. \ldots$

Hence the number of numbers of the form a which have, as exponent, a power of $p \ngtr p^s$, is $p^{(\Sigma n)_s}$ (using the notation of Proposition 23).

Hence the number of numbers, with exponent p^s generated by the numbers Γ, is

$$p^{(\Sigma n)_s} - p^{(\Sigma n)_{s-1}},$$

and, therefore, we must have

$$p^{(\Sigma n)_s} - p^{(\Sigma n)_{s-1}} = p^{(\Sigma l)_s} - p^{(\Sigma l)_{s-1}},$$

for all values of s from 1 up to the greatest of the values of the numbers l.

Hence we get

$$(\Sigma n)_1 = (\Sigma l)_1,$$
$$(\Sigma n)_2 = (\Sigma l)_2,$$
$$(\Sigma n)_3 = (\Sigma l)_3,$$
&c.

The first of these equations shows that the number of numbers l is the same as that of the numbers n.

The second then shows that, of each set, the number of numbers which exceed 1 is the same.

The third then shows that, of each set, the number of numbers which exceed 2 is the same.

And so on.

Hence the two sets of numbers $l_1, l_2, \ldots$ and $n_1, n_2, \ldots$ *are identical* (in some order) *term for term.*

We have, therefore, shown that the most general set of p-power-exponent generators must have as exponents the powers of $p, p^{l_1}, p^{l_2}, \ldots$, which occur, one each, as a principal factor of $\phi(P_1^{\lambda_1}), \phi(P_2^{\lambda_2}) \ldots$

When $p = 2$ we have the special case of the 2-power-exponent generators.

First suppose $\kappa' \geqq 1$, then

$$2^{(\Sigma\kappa)_\sigma + 1} - 2^{(\Sigma\kappa)_{\sigma-1} + 1} = 2^{(\Sigma n)_\sigma} - 2^{(\Sigma n)_{\sigma - 1}},$$

and so

$$(\Sigma\kappa)_1 + 1 = (\Sigma n)_1,$$
$$(\Sigma\kappa)_2 + 1 = (\Sigma n)_2,$$
&c.

Hence the set of numbers n are identical with the set κ *together with unity:* and so the exponents of the 2-power-exponent generators are

$$2.\ 2^{\kappa'}.\ 2^{\kappa_1}.\ 2^{\kappa_2}.\ \ldots$$

Secondly, suppose $\kappa = 2$, then $\kappa' = 0$, and the exponents of the generators are

$$2.\ 2^{\kappa_1}.\ 2^{\kappa_2}.\ \ldots$$

Lastly, when $\kappa = 0$ or 1, we have

$$2^{(\Sigma\kappa)_\sigma} - 2^{(\Sigma\kappa)_\sigma - 1} = 2^{(\Sigma n)_\sigma} - 2^{(\Sigma n)_\sigma - 1},$$

and therefore

$$\begin{aligned}(\Sigma\kappa)_1 &= (\Sigma n)_1,\\ (\Sigma\kappa)_2 &= (\Sigma n)_2,\\ &\text{\&c.,}\end{aligned}$$

and so the numbers n are identical with the numbers κ.

Hence the exponents of the 2-power-exponent generators are

$$2^{\kappa_1},\ 2^{\kappa_2},\ 2^{\kappa_3} \ldots$$

We can now see the least possible number of numbers G that can generate the complete set of $\phi(m)$ numbers.

Since each number G contains not more than one generator from each of the subsidiary sets of generators as a factor, it follows that there cannot be less generators G than the number of generators in that subsidiary set which contains most.

Now, since $\phi(P_1^{\lambda_1}) = P^{\lambda_1 - 1}(P_1 - 1)$, and P_1 is odd, therefore $P_1 - 1$ is even. Hence $\kappa_1 = 1$ at least. Therefore of the generators of the 2-power-exponent numbers there are at least as many as there are odd principal factors $P_1^{\lambda_1}$, $P_2^{\lambda_2}, \ldots$, in m: and so the number of 2-power-exponent generators is never less than the number of generators in any other subsidiary set.

Therefore when

$$\begin{array}{lr} & m = \left.\begin{array}{r} P_1^{\lambda_1}, \ldots \\ 2.P_1^{\lambda_1}, \ldots \end{array}\right\} \\ \text{or} & \end{array}$$

the least number of generators G is the number of primes P_1, when

$$m = 2^2.P_1^{\lambda_1}, \ldots$$

the least number of generators G is the number of primes P_1, + 1, and when

$$m = 2^{\kappa' + 2}P_1^{\lambda_1}, \ldots$$

the least number of generators G is the number of primes P_1, + 2.

(27.) We shall next form a set of p-power-exponent generators of a particular kind, similar to the complete generators of Proposition (24).

Let a be any p-power-exponent number

$$a \equiv \alpha_0\xi_0 + \alpha_1\xi_1 + \alpha_2\xi_2 + \ldots \pmod{m}.$$

Then we must have

$\alpha_0 \equiv 1 \pmod{2^\kappa}$
α_1 with exp a power of p (or unity) mod $P_1^{\lambda_1}$
α_2 ,, ,, p ( ) mod $P_2^{\lambda_2}$
&c.

Let

γ_1 be a number with exp p^{l_1} mod $P_1^{\lambda_1}$
γ_2 ,, ,, p^{l_2} mod $P_2^{\lambda_2}$,
&c.,

(if in any case p is not a factor of $\phi(P^\lambda)$ γ is $\equiv 1$).

Then we may put

$\alpha_1 \equiv \gamma_1^{i_1} \pmod{P_1^{\lambda_1}}$
$\alpha_2 \equiv \gamma_2^{i_2} \pmod{P_2^{\lambda_2}}$,
&c.,

and therefore

$$a \equiv \xi_0 + \gamma_1^{i_1}\xi_1 + \gamma_2^{i_2}\xi_2 + \ldots \pmod{m}$$

$$a \equiv (\xi_0 + \xi_1 + \ldots)(\xi_0 + \gamma_1\xi_1 + \ldots)^{i_1}(\xi_0 + \xi_1 + \gamma_2\xi_2 + \ldots)^{i_2} \ldots \pmod{m}$$

$$\equiv g_1^{i_1} g_2^{i_2} \ldots \pmod{m}.$$

The first factor and each of the following in which the γ is $= 1$ is $\equiv 1 \pmod{m}$.

The number of factors remaining is the number of the principal factors P^λ which have a power of p as a factor of $\phi(P^\lambda)$.

These factors generate the p-power-exponent numbers: corresponding to each set of indices i is one of the numbers a and *vice versâ.*

These generators are only a very special kind of p-power-exponent generators inasmuch as each is congruent to unity for each but one of the principal factors of m as modulus. They will be called unitary generators and will be useful for the discussion of the more general type.

In the case when $p = 2$, let

f be $\equiv 2^\kappa - 1$ or $2^{\kappa-1} - 1 \pmod{2^\kappa}$
γ_0 have exp $2^{\kappa-2} \pmod{2^\kappa}$

(if $\kappa = 2$, f does not occur; if $\kappa = 0$ or 1, neither g nor f),

γ_1 have exp $2^{\kappa_1} \pmod{P_1^{\lambda_1}}$
γ_2 ,, $2^{\kappa_2} \pmod{P_2^{\lambda_2}}$,
&c.,

and thus

$$a \equiv (f\xi_0 + \xi_1 + \ldots)^{j} (\gamma_0\xi_0 + \xi_1 + \ldots)^{i_0} (\xi_0 + \gamma_1\xi_1 + \ldots)^{i_1} \ldots \pmod{m},$$

and all the factors in this product (omitting those whose γ is $= 1$) form a complete set of 2-power-exponent generators.

Thus, in either case, when p is an odd prime or is equal to 2 we can form a set of p-power-exponent generators (having the exponents found to be necessary in Proposition 26), such that each is congruent to unity for all but one of the principal factors of m.

Example.—Let

$$m = 308 = 2^2.\ 7.\ 11.$$

$$\phi(m) = (2).\ (2.\ 3)\ (2.\ 5).$$

The highest exponent is 30.

There are

$$\left.\begin{array}{l} 7 \text{ numbers with exp } 2 \\ 1 \quad\text{,,}\qquad\quad\text{,,}\quad 1 \end{array}\right\} \text{(Example Proposition 26.)}$$

and

We will form unitary generators of these eight numbers. Since 2 enters only in the *square* into m, f is not needed.

We must take

$$\gamma_0 = 3 \text{ (with exp 2 mod } 2^2\text{)},$$
$$\gamma_1 = 6 \text{ (with exp 2 mod 7)},$$
$$\gamma_2 = 10 \text{ (with exp 2 mod 11)}.$$

$$\xi_0 = 77, \qquad \xi_1 = 176, \qquad \xi_2 = 56.$$

Thus

$$\left.\begin{array}{l} g_0 \equiv (\ 3 - 1)\ \ 77 + 1 = 155 \pmod{308} \\ g_1 \equiv (\ 6 - 1)\ 176 + 1 = 881 \equiv 265 \pmod{308} \\ g_2 = (10 - 1)\ \ 56 + 1 = 505 \equiv 197 \pmod{308} \end{array}\right\}$$

are a (in this case *the*) set of 2-power-exponent unitary generators.

The numbers with exponent 2 are given as products of powers of these by the following table of indices.

Numbers.	197.	265.	155.	111.	43.	153.	307.
Index of 155 . . .	0	0	1	1	1	0	1
Index of 265 . . .	0	1	0	1	0	1	1
Index of 197 . . .	1	0	0	0	1	1	1

(28.) In what follows we shall need the following lemma.

Consider

$$\begin{aligned} a_1x + b_1y + c_1z + \ldots &\equiv k_1 \pmod{p^\alpha} \\ a_2x + b_2y + c_2z + \ldots &\equiv k_2 \pmod{p^\alpha} \\ a_3x + b_3y + c_3z + \ldots &\equiv k_3 \pmod{p^\alpha} \\ \ldots\ldots\ldots\ldots &\ldots\ldots \end{aligned}$$

as many congruences as unknown quantities.

What is necessary in order that the congruences may have one solution, for any assigned set of values of the k's, and *one only*?

Multiply the equations in order by the minors of the elements of the 1st column of the determinant

$$\begin{vmatrix} a_1 & b_1 & c_1 & . \\ a_2 & b_2 & c_2 & . \\ a_3 & b_3 & c_3 & . \\ . & . & . & . \end{vmatrix} \text{ and add.}$$

We get

$$x \begin{vmatrix} a_1 & b_1 & c_1 & . \\ a_2 & b_2 & c_2 & . \\ a_3 & b_3 & c_3 & . \\ . & . & . & . \end{vmatrix} \equiv \begin{vmatrix} k_1 & b_1 & c_1 & . \\ k_2 & b_2 & c_2 & . \\ k_3 & b_3 & c_3 & . \\ . & . & . & . \end{vmatrix} \pmod{p^\alpha}.$$

In order that this may have one solution, and one only, the determinant

$$\begin{vmatrix} a_1 & b_1 & c_1 & . \\ a_2 & b_2 & c_2 & . \\ a_3 & b_3 & c_3 & . \\ . & . & . & . \end{vmatrix}$$

must be prime to p^α, and, therefore, prime to p.

This being so, then to each set of values of the k's corresponds a single set of values of $x, y, z. \ldots$

(29.) We have now to find the most general type of a set of p-power-exponent generators. (The work is in no respect different in the case when $p = 2$.)

Let the exponents necessary for a set of generators be $p^{l_1}, p^{l_2}, \ldots p^{l_\mu}$ as determined by Proposition (26).

Let

$$\left.\begin{array}{l} g_1 \text{ with exp. } p^{l_1} \\ g_2 \quad ,, \quad ,, \quad p^{l_2} \\ \vdots \\ g_\mu \quad ,, \quad ,, \quad p^{l_\mu} \end{array}\right\} \text{be a set of } \textit{unitary} \text{ generators. (Proposition 27.)}$$

Suppose that $\Gamma_1, \Gamma_2, \ldots \Gamma_\mu$ are the most general set of p-power-exponent generators. We know already (Proposition 27) that their exponents are p^{l_1}, p^{l_2}, . . . and we may suppose them to be so in this order.

Since each number Γ is itself a p-power-exponent number, each is expressible as a product of powers of the g's.

Let

$$\left.\begin{array}{l} \Gamma_1 \equiv g_1^{i_{11}} g_2^{i_{21}} g_3^{i_{31}} \ldots g_\mu^{i_{\mu 1}} \pmod{m} \\ \Gamma_2 \equiv g_1^{i_{12}} g_2^{i_{22}} g_3^{i_{32}} \ldots g_\mu^{i_{\mu 2}} \pmod{m} \\ \vdots \\ \Gamma_\mu \equiv g_1^{i_{1\mu}} g_2^{i_{2\mu}} g_3^{i_{3\mu}} \ldots g_\mu^{i_{\mu\mu}} \pmod{m} \end{array}\right\}$$

(*Note.*—$i_{r,s}$, is the index of g_r in the value of Γ_s.)

Since the exponent of Γ_1 is p^{l_1}, it follows that p^{l_1} is the least multiplier that makes

$$i_{21} p^{l_1} \equiv 0 \pmod{p^{l_2}},$$
$$i_{31} p^{l_1} \equiv 0 \pmod{p^{l_2}},$$
&c.,

(Proposition 8, Corollary), and similarly for p^{l_2}, &c.

We may insert here a lemma, which will be useful presently.

Lemma.—If $l_r > l_s$, then i_{rs} is divisible by p.

$$i_{rs} \text{ is the index of } g_r \text{ in the product } \Gamma_s,$$
$$\Gamma_s \equiv \ldots g_r^{i_{rs}} \ldots \pmod{m}.$$

Hence (Proposition 8, Corollary) the exponent of Γ_s is $\nless$ exponent of $g_r^{i_{rs}}$.

Suppose, if possible, that i_{rs} can be prime to p.

Then the exponent of $g_r^{i_{rs}}$ is p^{l_r} (Proposition 4).

Now the exponent of Γ_s is p^{l_s},

therefore

$$p^{l_s} \nless p^{l_r},$$

therefore

$$l_s \nless l_r,$$

which is contrary to the supposition $l_s < l_r$, and therefore i_{rs} cannot be prime to p.

Hence, if $l_r > l_s$, then i_{rs} is divisible by p.

Take any one whatever of the p-power-exponent numbers, $g_1^{I_1} g_2^{I_2} \ldots g_\mu^{I_\mu}$ (modulus m). Then, since the numbers Γ are also generators of these numbers (the p-power-exponent numbers), the numbers $g_1^{I_1} g_2^{I_2} \ldots g_\mu^{I_\mu}$ (modulus m) must be expressible in the form $\Gamma_1^{x_1} \Gamma_2^{x_2} \ldots \Gamma_\mu^{x_\mu}$ (modulus m) in one way, and one way only.

Therefore

$$g_1^{I_1} g_2^{I_2} \ldots g_\mu^{I_\mu} \equiv \Gamma_1^{x_1} \Gamma_2^{x_2} \ldots \Gamma_\mu^{x_\mu} \pmod{m}$$

must lead to

$$\begin{array}{l} \text{one value of } x_1 \pmod{p^{l_1}}, \\ \quad ,, \qquad ,, \quad x_2 \pmod{p^{l_2}}, \\ \&\text{c.} \end{array}$$

Substituting the values of the Γ's in terms of the g's,

$$(g_1^{i_{11}} g_2^{i_{21}} \ldots g_\mu^{i_{\mu 1}})^{x_1} (g_1^{i_{12}} g_2^{i_{22}} \ldots g_\mu^{i_{\mu 2}})^{x_2} \ldots (g_1^{i_{1\mu}} g_2^{i_{2\mu}} \ldots g_\mu^{i_{\mu\mu}})^{x_\mu} \equiv g_1^{\mathrm{I}_1} g_2^{\mathrm{I}_2} \ldots g_\mu^{\mathrm{I}_\mu} \pmod{m},$$

$$g_1^{i_{11} x_1 + i_{12} x_2 + \ldots + i_{1\mu} x_\mu} \cdot g_2^{i_{21} x_1 + i_{22} x_2 + \ldots i_{2\mu} x_\mu} \ldots g_\mu^{i_{\mu 1} x_1 + i_{\mu 2} x_2 + \ldots i_{\mu\mu} x_\mu} \equiv g_1^{\mathrm{I}_1} g_2^{\mathrm{I}_2} \ldots g_\mu^{\mathrm{I}_\mu} \pmod{m}.$$

Therefore (Proposition 7) it follows that

$$\begin{array}{l} i_{11} x_1 + i_{12} x_2 + \ldots + i_{1\mu} x_\mu \equiv \mathrm{I}_1 \pmod{p^{l_1}}, \\ i_{21} x_1 + i_{22} x_2 + \ldots + i_{2\mu} x_\mu \equiv \mathrm{I}_2 \pmod{p^{l_2}}, \\ \vdots \\ i_{\mu 1} x_1 + i_{\mu 2} x_2 + \ldots + i_{\mu\mu} x_\mu \equiv \mathrm{I}_\mu \pmod{p^{l_\mu}}, \end{array}$$

and we need that these shall have *one* set of values of x_1 (modulus p^{l_1}), x_2 (modulus p^{l_2}), &c., . . . and only one.

This being so the numbers Γ will generate completely the p-power-exponent numbers.

We may suppose that the moduli $p^{l_1}, p^{l_2} \ldots$ are in ascending order of magnitude, so that $l_s \overline{\underset{<}{}} l_{s+1}$.

Suppose that

$$l_1 = l_2 = l_3 = \ldots = l_a < l_{a+1} = l_{a+2} = \ldots = l_b < l_{b+1} = l_{b+2} = \ldots = l_c < \&\text{c.} \ldots = l_\mu.$$

Any one of the unknowns x_s is to be found with regard to mod p^{l_s}.

We can write x_s in the form

$$x_s \equiv \xi_s + \xi_{sa} p^{l_a} + \xi_{sb} p^{l_b} + \xi_{sc} p^{l_c} + \ldots \pmod{p^{l_s}},$$

where

$$\left.\begin{array}{l} \xi_s < p^{l_a} \\ \xi_{sa} < p^{l_b - l_a} \\ \xi_{sb} < p^{l_c - l_b} \end{array}\right\}$$
$$\&\text{c.}$$

This substitution gives in particular,

$$\begin{array}{lll} x_1 & \equiv \xi_1 \pmod{p^{l_a}}. \\ x_2 & \equiv \xi_2 \pmod{p^{l_a}}. \\ \vdots & \quad \vdots \qquad \vdots \\ x_a & \equiv \xi_a \pmod{p^{l_a}}. \end{array}$$

$$
\begin{aligned}
x_{a+1} &\equiv \xi_{a+1} + \xi_{a+1.a}\, p^{l_a} \pmod{p^{l_b}}. \\
x_{a+2} &\equiv \xi_{a+2} + \xi_{a+2.a}\, p^{l_a} \pmod{p^{l_b}}. \\
&\vdots \\
x_b &\equiv \xi_b + \xi_{ba}\, p^{l_a} \pmod{p^{l_b}}. \\[1ex]
x_{b+1} &\equiv \xi_{b+1} + \xi_{b+1.a}\, p^{l_a} + \xi_{b+1.b}\, p^{l_b} \pmod{p^{l_c}}. \\
x_{b+2} &\equiv \xi_{b+2} + \xi_{b+2.a}\, p^{l_a} + \xi_{b+2.b}\, p^{l_b} \pmod{p^{l_c}}. \\
&\vdots \\
x_c &\equiv \xi_c + \xi_{ca}\, p^{l_a} + \xi_{cb}\, p^{l_b} \pmod{p^{l_c}}. \\
&\qquad \&\text{c.} \qquad\qquad \&\text{c.}
\end{aligned}
$$

First replace each modulus which exceeds p^{l_a} by p^{l_a}, and substitute the assumed values of the x's.

We get the μ congruences

$$
\begin{aligned}
i_{11}\xi_1 + i_{12}\xi_2 + \ldots + i_{1\mu}\xi_\mu &\equiv \mathrm{I}_1 \pmod{p^{l_a}}, \\
i_{21}\xi_1 + i_{22}\xi_2 + \ldots + i_{2\mu}\xi_\mu &\equiv \mathrm{I}_2 \pmod{p^{l_a}}, \\
\cdots\cdots\cdots\cdots&\cdots\cdots \\
i_{\mu 1}\xi_1 + i_{\mu 2}\xi_2 + \ldots + i_{\mu\mu}\xi_\mu &\equiv \mathrm{I}_\mu \pmod{p^{l_a}},
\end{aligned}
$$

and we need that these shall determine a single set of values for $\xi_1, \xi_2, \ldots \xi_\mu$ (mod p^{l_a}).

The necessary and sufficient condition is that the determinant

$$(i_{11}, i_{22}, i_{33}, \ldots i_{\mu\mu})$$

should be prime to p (Proposition 28).

Suppose that this is so, and that the numbers $\xi_1, \xi_2, \ldots \xi_\mu$ are determined.

When these values are substituted above, suppose that the values of the left-hand sides are $\mathrm{I}_1 - p^{l_a}\mathrm{I}'_1$, $\mathrm{I}_2 - p^{l_a}\mathrm{I}'_2$, &c. ... (where the negative signs are written for convenience in what follows, and $\mathrm{I}'_1, \mathrm{I}'_2, \ldots$ are therefore negative).

Next replace each modulus which exceeds p^{l_b} by p^{l_b}, and substitute the assumed values of the x's.

The first a congruences are already satisfied.

The rest give

$$
\begin{aligned}
\mathrm{I}_{a+1} - p^{l_a}\mathrm{I}'_{a+1} + p^{l_a}\left(i_{a+1.a+1}\,\xi_{a+1.a} + i_{a+1.a+2}\,\xi_{a+2.a} + \ldots + i_{a+1.\mu}\,\xi_{\mu a}\right) &\equiv \mathrm{I}_{a+1} \pmod{p^{l_b}}. \\
\mathrm{I}_{a+2} - p^{l_a}\mathrm{I}'_{a+2} + p^{l_a}\left(i_{a+2.a+1}\,\xi_{a+1.a} + i_{a+2.a+2}\,\xi_{a+2.a} + \ldots + i_{a+2.\mu}\,\xi_{\mu a}\right) &\equiv \mathrm{I}_{a+2} \pmod{p^{l_b}}. \\
\cdots\cdots\cdots\cdots\cdots\cdots&\cdots\cdots \\
\mathrm{I}_\mu - p^{l_a}\mathrm{I}'_\mu + p^{l_a}\left(i_{\mu.a+1}\,\xi_{a+1.a} + i_{\mu.a+2}\,\xi_{a+2.a} + \ldots\ i_{\mu\mu}\,\xi_{\mu a}\right) &\equiv \mathrm{I}_\mu \pmod{p^{l_b}}.
\end{aligned}
$$

Therefore.

$$
\begin{aligned}
&i_{a+1.a+1}\,\xi_{a+1.a} + i_{a+1.a+2}\,\xi_{a+2.a} + \ldots + i_{a+1.\mu}\,\xi_{\mu a} \equiv \mathrm{I}'_{a+1} \pmod{p^{l_b-l_a}}\\
&i_{a+2.a+1}.\xi_{a+1.a} + i_{a+2.a+2}\,\xi_{a+2.a} + \ldots + i_{a+2.\mu}\,\xi_{\mu a} \equiv \mathrm{I}'_{a+2} \pmod{p^{l_b-l_a}}\\
&\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\\
&i_{\mu.a+1}\,\xi_{a+1.a} + i_{\mu.a+2}.\xi_{a+2.a} + \ldots \quad i_{\mu\mu}\,\xi_{\mu a} \equiv \mathrm{I}'_{\mu} \pmod{p^{l_b-l_a}},
\end{aligned}
$$

and we need that these shall determine a single set of values of

$$\xi_{a+1.a},\ \xi_{a+2.a},\ \ldots\ \xi_{\mu a} \pmod{p^{l_b-l_a}}.$$

The necessary and sufficient condition is that the determinant

$$(i_{a+1,\,a+1},\ i_{a+2,\,a+2},\ \ldots\ i_{\mu\mu})$$

should be prime to p.

Suppose that this is so, and the numbers $\xi_{a+1,\,a}$, $\xi_{a+2.a}$, . . . $\xi_{\mu a}$ are determined: and suppose that when substituted above the values of the left-hand sides become $\mathrm{I}'_{a+1} - p^{l_b-l_a}\mathrm{I}''_{a+1}$, &c.

Next replace each modulus that exceeds p^{l_c} by p^{l_c}, and substitute again the values of x.

The first b congruences are now satisfied.

The rest give

$$
\begin{aligned}
&(\mathrm{I}_{b+1} - \mathrm{I}'_{b+1}p^{l_a}) + (\mathrm{I}'_{b+1} - \mathrm{I}''_{b+1}p^{l_b-l_a})\,p^{l_a} + p^{l_b}\,(i_{b+1.b+1}\,\xi_{b+1.b} + \ldots\ i_{b+1.\mu}\,\xi_{\mu b}) \equiv \mathrm{I}_{b+1} \pmod{p^{l_c}}\\
&(\mathrm{I}_{b+2} - \mathrm{I}'_{b+2}p^{l_a}) + (\mathrm{I}'_{b+2} - \mathrm{I}''_{b+2}p^{l_b-l_a})\,p^{l_a} + p^{l_b}\,(i_{b+2.b+1}\,\xi_{b+1.b} + \ldots\ i_{b+2.\mu}\,\xi_{\mu b}) \equiv \mathrm{I}_{b+2} \pmod{p^{l_c}}\\
&\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\\
&(\mathrm{I}_{\mu} - \mathrm{I}'_{\mu}p^{l_a}) \quad + (\mathrm{I}'_{\mu} - \mathrm{I}''_{\mu}p^{l_b-l_a}) \quad + p^{l_b}(i_{\mu.b+1}\,\xi_{b+1.b} \quad + \ldots\ i_{\mu\mu}\,\xi_{\mu b}) \equiv \mathrm{I}_{\mu} \pmod{p^{l_c}}.
\end{aligned}
$$

Therefore

$$
\begin{aligned}
&i_{b+1.b+1}\,\xi_{b+1.b} + i_{b+1.b+2}\,\xi_{b+2.b} + \ldots + i_{b+1.\mu}\,\xi_{\mu b} \equiv \mathrm{I}''_{b+1} \pmod{p^{l_c-l_b}}\\
&\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\\
&i_{\mu.b+1}\,\xi_{b+1.b} \quad + i_{\mu.b+2}\,\xi_{b+2.b} \quad + \ldots\ i_{\mu\mu}\,\xi_{\mu b} \qquad \equiv \mathrm{I}''_{\mu} \pmod{p^{l_c-l_b}},
\end{aligned}
$$

and we need that these shall determine a single set of values of

$$\xi_{b+1.b},\ \xi_{b+2,\,b},\ \ldots\ \xi_{\mu b} \pmod{p^{l_c-l_b}}.$$

The necessary and sufficient condition for this is that the determinant

$$(i_{b+1.b+1},\ i_{b+2,\,b+2},\ \ldots\ i_{\mu\mu})$$

should be prime to p.

These successive steps are to be continued until all the quantities ξ are determined. They, and therefore the numbers x will be determined uniquely, provided that the conditions that

$$\left.\begin{array}{l} (i_{11} \ldots i_{\mu\mu}) \\ (i_{a+1}\, i_{a+1}, \ldots i_{\mu\mu}) \\ (i_{b+1,\, b+1}, \ldots i_{\mu\mu}) \\ \quad \text{\&c.,} \end{array}\right\} \text{ shall all be prime to } p, \text{ are satisfied.}$$

When these conditions are satisfied the generators Γ generate the complete set of p-power-exponent numbers.

(30.) We have not yet seen whether the conditions just found are independent or not. We shall find that the first condition $(i_{11}, i_{22}, \ldots i_{\mu\mu})$ includes all the others; it may, however, be replaced by others of a similar kind, but practically simpler.

Let us write down the complete determinant and divide it into squares and rectangles thus :—

$$\begin{array}{ccccc|cc|c}
i_{11} & i_{12} & \ldots & i_{1a-1} & i_{1a} & i_{1a+1} & i_{1b} & \\
i_{21} & i_{22} & \ldots & i_{2.\,a-1} & i_{2a} & \vdots & & \\
\vdots & & & & & \vdots & & \text{\&c.} \\
i_{a-1.\,1} & i_{a-1.\,2} & \ldots & i_{a-1.\,a-1} & i_{a-1.\,a} & \vdots & & \\
i_{a1} & i_{a2} & \ldots & i_{a.\,a-1} & i_{aa} & i_{aa+1} & i_{ab} & \\
\hline
i_{a+1.\,1} & & \ldots & & i_{a+1.\,a} & i_{a+1.\,a+1} & i_{a+1.\,b} & \\
\vdots & & & & & \vdots & & \\
i_{b1} & & \ldots & & i_{ba} & i_{ba+1} & i_{bb} & \\
\hline
 & & \text{\&c.} & & & & &
\end{array}$$

For reference, we may name these squares and rectangles, thus :—

$$\begin{array}{c|c|cc}
(aa) & (ab) & (ac) & \\
\hline
(ba) & (bb) & (bc) & \text{\&c.} \\
\hline
(ca) & (cb) & (cc) & \\
\end{array}$$

$$\text{\&c.}$$

The lemma proved in the course of the last proposition (that if $l_r > l_s$, then i_{rs} is divisible by p), shows that every element i, which is found to the left and below the determinants (aa), (bb), (cc) . . . is divisible by p, *i.e.*, every element in

$$\begin{array}{c|c|c|c} & & & \\ \hline (ba) & & & \\ \hline (ca) & (cb) & & \\ \hline (da) & (db) & (dc) & \end{array}$$

&c.,

is divisible by p.

The complete determinant $(i_{11}, \dots i_{\mu\mu})$ can be expressed as the sum of products of pairs of complementary determinants, one of these in each such product being the determinant formed by any a rows taken from (aa), (ba), (ca) . . .

Now, any row taken from (ba), (ca), . . . has every element divisible by p. Hence, the only determinant formed by a rows taken from (aa), (ba), (ca), . . . which is not immediately divisible by p, is the determinant $(aa) = (i_{11}, \dots i_{aa})$.

Hence

$$(i_{11}, \dots i_{\mu\mu}) \equiv (i_{11}, \dots i_{aa})\,(i_{a+1.\,a+1} \dots i_{\mu\mu}) \pmod{p}.$$

Therefore, if $(i_{11} \dots i_{\mu\mu})$ is prime to p, then $(i_{11}, \dots i_{aa})$ and $(i_{a+1.\,a+1}, \dots i_{\mu\mu})$ are both prime to p (and *vice versâ*).

Again, take the determinant $(i_{a+1.\,a+1}, \dots i_{\mu\mu})$,

$$\begin{array}{c|c|c} (bb) & (bc) & \\ \hline (cb) & (cc) & \quad \&c. \\ \hline & & \end{array}$$

&c.

This can be expressed as a sum of products of determinants in the same way: one determinant in each product being formed by $(b - a)$ rows taken from (bb), (cb) . . . Of these, only (bb) is not immediately divisible by p.

Therefore

$$(i_{a+1.\,a+1}, \ldots i_{\mu\mu}) \equiv (i_{a+1.\,a+1}, \ldots i_{bb})\ (i_{b+1.\,b+1}, \ldots i_{\mu\mu}) \pmod{p},$$

and, since

$$(i_{a+1.\,a+1}, \ldots i_{\mu\mu}) \text{ is prime to } p,$$

therefore

$$(i_{a+1.\,a+1}, \ldots i_{bb}) \text{ and } (i_{b+1.\,b+1}, \ldots i_{\mu\mu}) \text{ are both prime to } p,$$

and so on.

Hence, as stated above, the single condition $(i_{11}, \ldots i_{\mu\mu})$ prime to p, includes all the other conditions found necessary in Proposition (29), and is therefore a necessary and sufficient condition that the numbers Γ (having the proper set of exponents) may completely generate the p-power-exponent numbers.

Also, this single condition may be replaced (with much advantage practically) by the equivalent set of conditions—

$$\left.\begin{array}{c} (i_{11}, \ldots i_{aa}) \\ (i_{a+1}, i_{a+1}, \ldots i_{bb}) \\ (i_{b+1}, i_{b+1}, \ldots i_{cc}) \\ \&c. \end{array}\right\} \text{all prime to } p.$$

(31.) We have now a complete series of methods for ascertaining whether a given set of numbers G can act as generators of the complete system of $\phi(m)$ numbers (modulus m).

(1.) Find the exponent to which each belongs. (Proposition 17.)

(2.) The principal factors of these exponents must be the numbers found in Proposition (26).

(3.) Express each number G as a product of numbers with principal factors of exponent of G as exponents. (Proposition 10.)

(4.) Express each of these last as a product of powers of unitary generators, and thus get for each a set of indices.

(5.) Apply the series of conditions of Proposition (30).

If (2) and (5) are both satisfied then the numbers G are complete generators.

Conversely to form any set of generators—

(1.) For each prime p in $\phi(m)$ form a set of unitary generators.

(2.) Form from these any set of p-power-exponent generators satisfying the conditions of Proposition 30.

(3.) Multiply together one generator from each of the sets just formed.

Examples.

Let us form a set of generators for mod $308 = 2^2.\ 7.\ 11.$

$$m = 2^2.\ 7.\ 11.$$
$$\phi(7) = 2.\ 3.$$
$$\phi(11) = 2.\ 5.$$

The principal factors of the exponents of the generators are

2. 2. 2. 3. 5.

We form first the numbers with exponent 2 to generate the 2-exponent numbers.

These numbers expressed in terms of the unitary generators, 155, 265, 197, are given by

No.	Ind. of 155.	Ind. of 265.	Ind. of 197.
197.	0.	0.	1.
265.	0.	1.	0.
155.	1.	0.	0.
111.	1.	1.	0.
43.	1.	0.	1.
153.	0.	1.	1.
307.	1.	1.	1.

Of these (by Proposition 30) we can take any three such that the determinant formed by their indices is prime to 2, *i.e.*, odd.

For example,

$$\begin{vmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{vmatrix} = -1,$$

and so 43, 153, 307 may be taken as generators.

Secondly we need a number with exponent 3.

Of these there are two, 177 and 221. Let us take 177.

Lastly we need a number with exponent 5.

Of these there are four, 113, 141, 169, 225. Let us take 113.

We have now 43, 153, 307, independent generators with exponent 2,

177 with exp 3,
113 ,, ,, 5.

These we may combine in any manner we please as products, taking only one from each set in each product.

Let us take $43.\ 177.\ 113 \equiv 107 \pmod{308}$ with exponent 30.

We have thus obtained three generators

$$\left.\begin{array}{l} 107 \text{ with exp } 30 \\ 153 \quad ,, \quad ,, \quad 2 \\ 307 \quad ,, \quad ,, \quad 2 \end{array}\right\}$$

which generate the complete set of $\phi(308)$ numbers.

Conversely, we can verify that 107. 153. 307 are complete generators.

First we find that

$$\left.\begin{array}{llll} 107 & \text{has} & \text{exp} & 30 \\ 153 & ,, & ,, & 2 \\ 307 & ,, & ,, & 2 \end{array}\right\}$$

and so the exponents have the necessary principal factors.

$$\begin{aligned} 107 &\equiv 107^{15}.\ 107^{10}.\ 107^{6} \pmod{308}, \\ &\equiv 43.\ 177.\ 113 \pmod{308}, \end{aligned}$$

where

$$\left.\begin{array}{llll} 43 & \text{has} & \text{exp} & 2 \\ 177 & ,, & ,, & 3 \\ 113 & ,, & ,, & 5 \end{array}\right\}$$

We only need to show that 43, 153, 307 are independent; and since the indices of these when referred to the unitary generators are

$$\begin{array}{rccc} 43, & 1 & 0 & 1 \\ 153, & 0 & 1 & 1 \\ 307, & 1 & 1 & 1 \end{array}$$

and the determinant is prime to 2, we see that the generators 43. 153. 307 are independent.

Let us form generators for modulus $999 = 3^3.\ 37$.

$$\begin{aligned} m &= 3^3.\ 37, \\ \phi(m) &= (3^2.\ 2)(3^2.\ 2^2). \end{aligned}$$

The principal factors of the exponents of the generators are

$$2.\ 2^2.\ 3^2.\ 3^2.$$

If

$$\begin{aligned} a &\equiv \alpha_1 \pmod{3^3}, \\ &\equiv \alpha_2 \pmod{37}, \\ a &\equiv \alpha_1\xi_1 + \alpha_2\xi_2 \pmod{3^3.\ 37}. \end{aligned}$$

$$\begin{aligned} 37x_1 &\equiv 1 \pmod{3^3} \\ 10x_1 &\equiv 1 \pmod{27} \\ x_1 &\equiv 19 \pmod{3^3} \\ \xi_1 &\equiv 37.\ 19 \equiv 703 \pmod{999} \end{aligned}$$

$$\begin{aligned} 27x_2 &\equiv 1 \pmod{37} \\ x_2 &\equiv 11 \pmod{37} \\ \xi_2 &\equiv 297 \pmod{999} \end{aligned}$$

and, therefore,

$$a \equiv 703\alpha_1 + 297\alpha_2 \pmod{999}.$$

We want first any number with exponent 2.

Suppose we take $\alpha_1 = 26$ and $\alpha_2 = 36$ each with exponent 2 (for moduli 3^3 and 37 respectively).

Then we get

$$\begin{aligned} a &\equiv 703.\ 26 + 297.\ 36 \pmod{999} \\ &\equiv 998 \pmod{999} \text{ with exp } 2. \end{aligned}$$

We want next a number with exponent 4.

Suppose we take

$$\alpha_1 = 1$$

and

$$\alpha_2 = 6 \text{ (with exp 4, mod 37).}$$

Then we get

$$\begin{aligned} a &\equiv 703 + 297.\ 6 \pmod{999} \\ &\equiv 487 \pmod{999} \text{ with exp } 4. \end{aligned}$$

Lastly, we want two independent generators with exponent 3^2.

We first form unitary generators with exponents 3^2

$$\alpha_1 = 4 \quad \alpha_2 = 1 \text{ gives } 112 \text{ with exp } 3^2,$$

and

$$\alpha_1 = 1 \quad \alpha_2 = 12 \text{ gives } 271 \text{ with exp } 3^2.$$

We may take for our 3-power-exponent generators any two numbers of the form $112^{i_1}\, 271^{i_2}$, $112^{i'_1}\, 271^{i'_2}$, provided that

$$\begin{vmatrix} i_1 & i_2 \\ i'_1 & i'_2 \end{vmatrix} \text{ is prime to 3.}$$

Suppose we take it

$$\begin{vmatrix} 1 & 1 \\ 2 & 1 \end{vmatrix}$$

and then the generators are

$$112.\ 271 \equiv 382 \pmod{999}$$

and

$$112^2.\ 271 \equiv 826 \pmod{999}.$$

Thus we have

998 with exp 2,
487 with exp 4,

and

$$382 \text{ and } 826 \text{ with exp } 3^2.$$

Hence we may form, say,

$$998.\ 826 \equiv 173 \pmod{999} \text{ with exp } 2.\ 3^2.$$

and

$$487.\ 382 \equiv 220 \pmod{999} \text{ with exp } 2^2.\ 3^2.$$

Thus

$$\left.\begin{array}{l} 173 \text{ with exp } 18 \\ 220 \text{ with exp } 36 \end{array}\right\}$$

generate completely the $2^3.\ 3^4$ numbers prime to 999.

INDICES AND TABLES OF INDICES.

(32.) Let $G_1\ G_2 \ldots G_\kappa$ be a complete set of independent generators for modulus m.

Let their exponents be $t_1, t_2, \ldots t_\kappa$.

Then any number a prime to m is expressible in the form

$$a \equiv G_1^{i_1}\ G_2^{i_2} \ldots G_\kappa^{i_\kappa} \pmod{m},$$

where

$$i_1 < t_1,\ i_2 < t_2, \text{ \&c.}$$

We may thus make a table giving the set of indices $i_1, i_2, \ldots i_\kappa$ which correspond to any number a, and conversely the number a which corresponds to any set of indices.

We may conveniently write

$$a \equiv (i_1, i_2, \ldots i_\kappa),$$

and then if

$$a' \equiv (i'_1, i'_2, \ldots i'_\kappa)$$

we shall have

$$aa' \equiv (i_1 + i'_1, i_2 + i'_2, \ldots i_\kappa + i'_\kappa)$$

and

$$a^s \equiv (i_1 s, i_2 s, \ldots i_\kappa s).$$

With tables of this kind for every modulus we can at once solve any congruence of the form

$$ax^n \equiv b \pmod{m}$$

whatever m may be, if a and b are both prime to m. For suppose that

$$a \equiv (i_1\ i_2 \ldots)$$

$$b \equiv (i'_1\ i'_2 \ldots)$$

$$x \equiv (I_1, I_2, \ldots)$$

Then we must have

$$i_1 + n\mathrm{I}_1 \equiv i'_1 \pmod{t_1}$$
$$i_1 + n\mathrm{I}_2 \equiv i'_2 \pmod{t_2},$$
&c.

The G.C.M. of n and t_1 must divide $i'_1 - i_1$, &c., in order that the congruences may be soluble.

These being so we find $\mathrm{I}_1, \mathrm{I}_2, \ldots$ by reference to tables with moduli $t_1, t_2, \ldots$ which are (or may be) composite numbers.

If

ν_1 is the G.C.M. of n and t_1, I_1 will have ν_1 values mod t_1,
ν_2 ,, ,, n and t_2, I_2 ,, ν_2 ,, t_2,
&c.

Hence, by reference again to the table for modulus m, we obtain at once the $\nu_1, \nu_2, \nu_3 \ldots$ numbers which satisfy the congruence $ax^n \equiv b \pmod{m}$.

Let us now solve the same congruence with the help only of tables of indices for powers of primes as moduli.

If

α_0 is a solution of the congruence $ax^n \equiv b \pmod{2^\kappa}$,
α_1 ,, ,, ,, $ax^n \equiv b \pmod{\mathrm{P}_1^{\lambda_1}}$,
&c.,

then

$$x \equiv \alpha_0\xi_0 + \alpha_1\xi_1 + \alpha_2\xi_2 \ldots \pmod{m}$$

is a solution of the congruence

$$ax^n \equiv b \pmod{m}.$$

Hence the solution is conducted as follows :—

By means of the tables of indices find

all the values α_0 which satisfy $ax^n \equiv b \pmod{2^\kappa}$,
,, ,, α_1 ,, ,, $\pmod{\mathrm{P}_1^{\lambda_1}}$,
&c.

Next find the values of the ξ's, Proposition (19), each being found by the tables.

Lastly the values of x which satisfy $ax^n \equiv b \pmod{m}$ must each be calculated separately by giving to each of $\alpha_0, \alpha_1, \ldots$ one of its possible values.

In the case of a multiple solution the labour involved in this last step may be very great; and consequently the saving of labour effected by the use of tables of indices for composite moduli proportionately so.

As an example of the use of tables of indices for composite moduli let us use the table given in the example to Proposition (24).

Solve

$$9x^5 \equiv 53 \pmod{112}.$$
$$53 \equiv (4.\ 1.\ 1.)$$

(written in this order the indices are referred to moduli 6. 4. 2),

$$9 \equiv (2.\ 2.\ 0),$$

and, therefore,

$$x^5 \equiv (2.\ 3.\ 1).$$

If, then,

$$x \equiv (a.\ b.\ c)$$
$$x^5 \equiv (5a.\ 5b.\ 5c),$$

and, therefore,

$$5a \equiv 2 \pmod 6, \text{ and, therefore, } a = 4,$$
$$5b \equiv 3 \pmod 4, \text{ and, therefore, } b = 3,$$
$$5c \equiv 1 \pmod 2, \text{ and, therefore, } c = 1,$$

therefore

$$x \equiv (4.\ 3.\ 1),$$
$$x \equiv 109 \pmod{112}.$$

Solve

$$47x^2 \equiv 55 \pmod{112}.$$
$$55 \equiv (3.\ 0.\ 1),$$
$$47 \equiv (5.\ 2.\ 1),$$

therefore

$$x^2 \equiv (4.\ 2.\ 0),$$

therefore, if

$$x \equiv (a.\ b.\ c)$$

$$\begin{array}{lll} 2a \equiv 4 \pmod 6, & 2b \equiv 2 \pmod 4, & 2c \equiv 0 \pmod 2, \\ a \equiv 2 \pmod 3, & b \equiv 1 \pmod 2, & c = 0 \text{ or } 1 \\ a = 2 \text{ or } 5. & b = 1 \text{ or } 3. & \end{array}$$

Hence there are eight solutions

$$\begin{array}{llll} (2\ \ 1\ \ 0) \equiv 51 & & (5\ \ 1\ \ 0) \equiv 19 \\ (2\ \ 1\ \ 1) \equiv 37 & & (5\ \ 1\ \ 1) \equiv 5 \\ (2\ \ 3\ \ 0) \equiv 107 & & (5\ \ 3\ \ 0) \equiv 75 \\ (2\ \ 3\ \ 1) \equiv 93 & & (5\ \ 3\ \ 1) \equiv 61. \end{array}$$

(33.) The last proposition shows how, by means of tables of indices for composite moduli, to solve (when possible) the congruence

$$ax^n \equiv b \pmod{m},$$

where m is any composite modulus and a and b are both prime to m.

To complete the question of the solution of the congruence for all cases we have now to show how it is solved when a and b are not both prime to m.

I. First, if a is not prime to m, the congruence can be at once reduced to the case in which it is so; for if a and m have G.C.M. κ, then κ must divide b, and we have

$$\left(\frac{a}{\kappa}\right) x^n \equiv \frac{b}{\kappa} \left(\bmod \frac{m}{\kappa}\right), \text{ where now } \frac{a}{\kappa} \text{ is prime to } \frac{m}{\kappa}\cdot$$

Any one solution x of this gives κ solutions of the original congruence $ax^n \equiv b \pmod{m}$, viz.,

$$x,\ x + \frac{m}{\kappa},\ x + \frac{2m}{\kappa}, \dots x + \overline{\kappa - 1}\,\frac{m}{\kappa}\cdot$$

II. We have now, therefore, only to deal with the congruence of the form $ax^n \equiv b \pmod{m}$, in which a is prime to m and b is not prime to m. Let κ be the G.C.M. of b and m, and express κ as the product of its principal factors $\kappa = p^r p'^{r'} \dots$

Since κ divides b and m, it divides ax^n.

Now a is prime to m, and therefore to κ; therefore κ divides x^n, *i.e.*, $p^r p'^{r'} \dots$ divides x^n. Therefore x is divisible by $p^\rho p'^{\rho'} \dots$ where

$$\begin{gathered} n\rho \geqq r, \\ n\rho' \geqq r', \\ \&\text{c.} \end{gathered}$$

Take ρ to be equal to r/n if r/n is an integer. If r/n is not an integer take ρ equal to the integer next greater.

Put

$$x = \xi p^\rho p'^{\rho'} \dots,$$

then the congruence

$$a\frac{x^n}{\kappa} \equiv \frac{b}{\kappa}\left(\bmod \frac{m}{\kappa}\right) \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad (\text{i.})$$

gives

$$a\left(p^{n\rho - r} p'^{n\rho' - r'} \dots\right) \xi^n \equiv \frac{b}{\kappa}\left(\bmod \frac{m}{\kappa}\right) \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad (\text{ii}).$$

If $n\rho - r \neq 0$ (*i.e.*, if r/n is not an integer), then the coefficient of ξ^n in this congruence is divisible by a power of p, and therefore, if the congruence is possible, m/κ is not (for then b/κ would be also, whereas m/κ and b/κ are co-prime).

Thus

$$p^{n\rho - r} p'^{n\rho' - r'} \ldots \text{ is prime to } m/\kappa,$$

and, therefore, since a and b/κ are also prime to m/κ, the congruence (ii.) is soluble (if possible) by means of the tables giving the indices of numbers prime to the modulus.

Each solution ξ of the congruence (ii.) gives a single solution $x \equiv \xi p^{\rho} p'^{\rho'} \ldots$ (mod m) of the congruence $ax^n \equiv b \pmod{m}$.

Example.—Solve

$$22x^5 \equiv 54 \pmod{672}.$$

The congruence is

$$2.\ 11.\ x^5 \equiv 2.\ 3^3 \pmod{2^5.\ 3.\ 7} \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad (\text{i.})$$

Dividing by 2 we have

$$11.\ x^5 \equiv 3^3 \pmod{2^4.\ 3.\ 7} \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad (\text{ii.})$$

and any solution x of this gives the two solutions x, $x + 336$ of the congruence (i.).

From (ii.) we get, dividing by 3,

$$11 \frac{x^5}{3} \equiv 9 \pmod{2^4.\ 7}.$$

In congruence (ii.) let $x = 3\xi$.

Then

$$11.\ 3^4.\ \xi^5 \equiv 9 \pmod{2^4.\ 7}$$

$$11.\ 3^2.\ \xi^5 \equiv 1 \pmod{2^4.\ 7}.$$

Now (see table, p. 222)

$$11 \equiv (4.\ 3.\ 0),$$

$$9 \equiv (2.\ 2.\ 0),$$

therefore

$$9.\ 11 \equiv (0.\ 1.\ 0),$$

therefore

$$\xi^5 \equiv (0.\ 3.\ 0),$$

therefore

$$\xi \equiv (0.\ 3.\ 0)$$

$$\xi \equiv 43 \pmod{2^4.\ 7}.$$

Hence (ii.) has the solution

$$x \equiv 129 \pmod{336},$$

and therefore the solutions of (i.) are

$$x \equiv 129,\ 465 \pmod{672}.$$

PART II.—ON THE RESIDUES OF POWERS OF NUMBERS FOR ANY MODULUS, COMPOSITE AND COMPLEX.

In order to maintain as far as possible the parallelism of Parts I. and II. a number of facts and relations peculiar to complex numbers are noted (most without proof) in the following Preface to Part II.

Preface to Part II.

Complex primes.—*i.e.*, numbers either real or complex which have no real or complex factors.

These are of two kinds

(i.) Real primes of the form $4k + 3$; *e.g.* 3, 7, 11, 19, . . .

(ii.) The factors of real primes of the form $4k + 1$, which are expressible as the sum of two squares, *e.g.*, $1 + 2i$, $2 + i$, $3 + 2i$, $2 + 3i$ . . . Among the last we include the factors of the real prime 2, viz., $1 + i$.

These two kinds of prime we shall call respectively *pure* and *mixed*, speaking of either as a *complex* prime. By a real prime we shall mean the primes ordinarily so called, real numbers which have no real factors.

To express any number as a product of its prime factors.

Let $a + bi$ be the number. Let d be the G.C.M. of a and b, and suppose that

$$a + bi = d(\alpha + \beta i).$$

d is a real number and can be expressed as a product of real primes.

Of these, those that are not complex primes can be separated each into its two factors.

All the factors of $\alpha^2 + \beta^2$ are themselves expressible as the sum of two squares.

Say

$$\alpha^2 + \beta^2 = (\alpha_1^2 + \beta_1^2)(\alpha_2^2 + \beta_2^2) \ldots$$

Then the prime factors of $\alpha + \beta i$ are

$$\alpha_1 \pm i\beta_1,$$
$$\alpha_2 \pm i\beta_2, \ldots$$

where, in each pair, the sign must be so chosen that

$$\alpha + \beta i = (\alpha_1 \pm i\beta_1)(\alpha_2 \pm i\beta_2) \ldots$$

Example.

$$60 + 105i = 15(4 + 7i)$$

$$15 = 3.\ 5 = 3(2 + i)(2 - i)$$

$$4^2 + 7^2 = 65 = 5.\ 13 = (2^2 + 1^2)(3^2 + 2^2)$$

and

$$4 + 7i = (2 + i)\,(3 + 2i)$$

therefore

$$60 + 105i = 3\,(2 - i)\,(2 + i)^2\,(3 + 2i).$$

The number of incongruent residues for any modulus m.

The number of incongruent residues (including zero) is the *norm* of the modulus. Thus if $m = \alpha + \beta i$, the number of incongruent residues modulus m is $\alpha^2 + \beta^2$. When the modulus is a pure number, $m = p$, then the number of incongruent residues is p^2.

Set of numbers all incongruent for modulus m.

Let $m = d\,(\alpha + \beta i)$ where α and β are co-prime.

Then the $N\,(m) = d^2\,(\alpha^2 + \beta^2)$ numbers $x + iy$, where x has any one of the values $0, 1, 2, \ldots d\,(\alpha^2 + \beta^2) - 1$, and y any one of the values $0, 1, 2, 3, \ldots \overline{d - 1}$, are a complete set of $N\,(m)$ incongruent residues for mod m.

We have two special cases:—

(i.) If $m = \alpha + \beta i$, the residues are $0, 1, 2, \ldots \alpha^2 + \beta^2 - 1$.

(ii.) If $m = d$, the residues are the numbers $x + iy$, where x and y have each any one of the values $0, 1, 2, \ldots \overline{d - 1}$.

For most purposes the above set of residues are most convenient. It is sometimes, however, a saving of arithmetical labour (in examples) to make use of the "absolutely least residues," *i.e.*, the set of residues whose norms are not greater than half the norm of the modulus. We may also make use of "least positive residues," *i.e.*, the set of numbers whose norms are as small as possible consistently with each number having both its parts positive.

In what follows we shall always use the above set of residues and we shall need an expeditious method for finding to which of them any given number is congruent.

To reduce a number to its residue.

Let $X + iY$ be the number whose residue we wish to find for mod $d\,(\alpha + \beta i)$, where α and β are co-prime.

We have to find x and y so that

$$X + iY \equiv x + iy \pmod{d\,\overline{\alpha + \beta i}},$$

where

$$\left.\begin{aligned} x &< d\,(\alpha^2 + \beta^2) \\ y &< d \end{aligned}\right\}\text{and both are positive numbers.}$$

Let

$$X + iY = (x + iy) + (\xi + i\eta)\,(\alpha + \beta i)\,d.$$

Then

$$\begin{aligned} X &= x + d\,(\alpha\xi - \beta\eta) \\ Y &= y + d\,(\beta\xi + \alpha\eta). \end{aligned}$$

The second equation gives $y \equiv Y \pmod{d}$, which determines y.
Then

$$\beta\xi + \alpha\eta = \frac{Y - y}{d},$$

α and β are co-prime, and therefore we can find α' and β' so that $\alpha'\beta - \alpha\beta' = 1$, and then

$$\left.\begin{aligned} \xi &= \alpha' \frac{Y-y}{d} + \lambda\alpha \\ \eta &= -\beta' \frac{Y-y}{d} - \lambda\beta \end{aligned}\right\} \text{where } \lambda \text{ is some integer.}$$

Therefore,

$$\begin{aligned} X &= x + d\left[\frac{Y-y}{d}(\alpha\alpha' + \beta\beta') + \lambda\,(\alpha^2 + \beta^2)\right] \\ &= x + (Y - y)\,(\alpha\alpha' + \beta\beta') + \lambda\,.\,d\,(\alpha^2 + \beta^2), \end{aligned}$$

and therefore

$$x \equiv X - (Y - y)\,(\alpha\alpha' + \beta\beta') \pmod{d\,.\,\overline{\alpha^2 + \beta^2}},$$

which determines x.

So x and y are given by

$$\begin{aligned} y &\equiv Y \pmod{d} \\ x &\equiv X - (Y - y)\,(\alpha\alpha' + \beta\beta') \pmod{d\,.\,\alpha^2 + \beta^2} \end{aligned}$$

where $\alpha\alpha' + \beta\beta'$ is a constant depending on the modulus.

Example.

Mod 3 (3 + 2i)

$$d = 3. \qquad \left.\begin{matrix} \alpha = 3 & \beta = 2 \\ \alpha' = -1 & \beta' = -1 \end{matrix}\right\} \alpha\alpha' + \beta\beta' = -5.$$

The reducing formulæ are

$$\begin{aligned} y &\equiv Y \pmod{3} \\ x &\equiv X + 5\,(Y - y) \pmod{39}. \end{aligned}$$

Thus to find the residues of the successive powers of $1 + i$:—

$$\begin{aligned}
& 1 + i \\
& 2i \\
-2 + 2i &\equiv 37 + 2i \\
35 + 39i &\equiv 35 \\
35 + 35i &\equiv 5 + 2i \\
3 + 7i &\equiv 33 + i \\
32 + 34i &\equiv 2 + i \\
1 + 3i &\equiv 16 \\
16 + 16i &\equiv 13 + i \\
12 + 4i &\equiv 33 + 2i \\
31 + 35i &\equiv 1 + 2i \\
-1 + 3i &\equiv 14 \\
14 + 14i &\equiv 35 + 2i \qquad (\text{mod } 9 + 6i) \\
33 + 37i &\equiv 18 + i \\
17 + 19i &\equiv 29 + i \\
28 + 30i &\equiv 22 \\
22 + 22i &\equiv 10 + i \\
9 + 11i &\equiv 15 + 2i \\
13 + 17i &\equiv 10 + 2i \\
8 + 12i &\equiv 29 \\
29 + 29i &\equiv 8 + 2i \\
6 + 10i &\equiv 12 + i \\
11 + 13i &\equiv 32 + i \\
31 + 33i &\equiv 1
\end{aligned}$$

In the two special cases

(i.) $m = \alpha + \beta i$

$$X + iY \equiv x \ (\text{mod } \alpha + \beta i) \quad \text{and} \quad x$$

is determined by

$$x \equiv X - Y\,(\alpha\alpha' + \beta\beta')\ (\text{mod } \alpha^2 + \beta^2).$$

(ii.) $m = d$

$$X + iY \equiv x + iy \ (\text{mod } d) \quad \text{and} \quad x \quad \text{and} \quad y$$

are given by

$$x \equiv X \ (\text{mod } d),$$

$$y \equiv Y \ (\text{mod } d).$$

Number of residues prime to any modulus.

Let the modulus be expressed as a product of powers of its prime factors, $m = p^\alpha q^\beta \ldots$ then of the N (m) residues,

$$\Phi(m) = [\mathrm{N}(p^\alpha) - \mathrm{N}(p^{\alpha-1})]\,[\mathrm{N}(q^\beta) - \mathrm{N}(q^{\beta-1})] \ldots$$

are prime to m.

In particular for a pure prime p,

$$\Phi(p) = p^2 - 1 \quad \text{and} \quad \Phi(p^\alpha) = p^{2\alpha} - p^{2\alpha-2};$$

and for a mixed prime, $a + bi$,

$$\Phi(a + bi) = a^2 + b^2 - 1 \quad \text{and} \quad \Phi(a + bi)^\alpha = (a^2 + b^2)^\alpha - (a^2 + b^2)^{\alpha-1}.$$

This value Φ, when we are dealing with complex numbers, must be distinguished from the value ϕ when we are concerned only with real numbers.

To a mixed prime ϕ is inapplicable, and to a real it has the relations $\phi(p) = p - 1$, $\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

Any modulus may be multiplied by -1, i, *or* $-i$, for if the modulus is a factor of any number it remains a factor on being multiplied by -1, i, or $-i$. This enables us to change any modulus into one entirely positive :—

For

$$\left.\begin{aligned} -\alpha - \beta i &= -1(\alpha + \beta i) \\ -\beta + \alpha i &= i(\alpha + \beta i) \\ \beta - \alpha i &= -i(\alpha + \beta i) \end{aligned}\right\}.$$

PART II.—RESIDUES OF POWERS OF NUMBERS FOR ANY MODULUS, COMPOSITE AND COMPLEX.

(i.) a being a number prime to m each term of the series of residues

$$a, a^2, a^3, \ldots \pmod{m}$$

is one of the $\Phi(m)$ residues which are prime to m. Hence, as in (Proposition 1), we see that, if t is the smallest integer for which $a^t \equiv 1 \pmod{m}$, the infinite series of residues consists of a repetition of t terms beginning from the first term. The number t is called the exponent of a for the modulus m.

Example.—The series of residues of the first twenty-four powers of the number $2 + i$ for the modulus 9 are

$$\begin{array}{r}
2 + i \\
3 + 4i \\
2 + 2i \\
2 + 6i \\
7 + 5i \\
8i \\
1 + 7i \\
4 + 6i \\
2 + 7i \\
6 + 7i \\
5 + 2i \\
8 \phantom{{}+ 0i} \\
7 + 8i \\
6 + 5i \\
7 + 7i \\
7 + 3i \\
2 + 4i \\
i \\
8 + 2i \\
5 + 3i \\
7 + 2i \\
3 + 2i \\
4 + 7i \\
1 \phantom{{}+ 0i}
\end{array}$$

after which the set of twenty-four terms constantly repeats itself.

(ii.) The proof is identical with 2, that if a has exponent t mod m and $a^s \equiv 1$, then t divides s.

(iii.) The proof of FERMAT'S theorem $a^{\Phi(m)} \equiv 1$ (mod m) is identical with that in (3) if for "the $\phi(m)$ numbers less than m and prime to it," we substitute "the $\Phi(m)$ residues of m that are prime to it."

Hence the corollary, that the exponent of any number, modulus m, is a divisor of $\Phi(m)$.

Example.—Mod $9 = 3^2$. $\Phi(3^2) = 3^4 - 3^2 = 72$. In Proposition (i.) we saw that the exponent of $2 + i$, mod 9, is 24, a divisor of 72.

(iv.) The proof is identical with that of (4). If a has exponent t, mod m, then a^s has exponent τ: where $t = \kappa\tau$ and κ is the G.C.M. of s and t.

Example.—Taking again the successive powers of $2 + i$, mod 9, we find the exponent of each of the twenty-four numbers.

No.	s.	τ = exp.
$2 + i$	1	24
$3 + 4i$	2	12
$2 + 2i$	3	8
$2 + 6i$	4	6
$7 + 5i$	5	24
$8i$	6	4
$1 + 7i$	7	24
$4 + 6i$	8	3
$2 + 7i$	9	8
$6 + 7i$	10	12
$5 + 2i$	11	24
8	12	2
$7 + 8i$	13	24
$6 + 5i$	14	12
$7 + 7i$	15	8
$7 + 3i$	16	3
$2 + 4i$	17	24
i	18	4
$8 + 2i$	19	24
$5 + 3i$	20	6
$7 + 2i$	21	8
$3 + 2i$	22	12
$4 + 7i$	23	24
1	24	1

(v.) The proof is the same as that of (5).

If the exponent of a is t, and of a' is t', and t and t' are co-prime, then the exponent of aa' is tt'.

And hence the corollary, that the same is true for any number of numbers: if $a, a', a'', \ldots$ have exponents $t, t', t'', \ldots$ co-prime, then $aa'a'' \ldots$ has exponent $tt't'' \ldots$

Example.—The exponent of 3 for mod $1 + 5i$ is 3.

Its successive powers have residues 3. 9. 1.

The exponent of 5 for mod $1 + 5i$ is 4.

Its successive powers have residues 5. 25. 21. 1.

Hence the exponent of $5 \times 3 = 15$ is $4 \times 3 = 12$.

The successive powers of 15 have residues 15. 17. 21. 3. 19. 25. 11. 9. 5. 23. 7. 1.

Example.—The exponent of 2, mod 7, is 3. The residues are 2. 4. 1.

The exponent of $5 + 2i$ is 8. The residues are $5 + 2i$, $6i$, $2 + 2i$, 6, $2 + 5i$, i, $5 + 5i$, 1.

Hence the exponent of $10 + 4i \equiv 3 + 4i$ is $3 \times 8 = 24$.

The successive residues are

$3 + 4i$	$3i$	$2 + 2i$	5	$1 + 6i$	i.
$3 + 3i$	4	$5 + 2i$	$5i$	$1 + i$	6.
$4 + 3i$	$4i$	$5 + 5i$	2	$6 + i$	$6i$.
$4 + 4i$	3	$2 + 5i$	$2i$	$6 + 6i$	1.

(vi.) The proof is the same as for (6).

Suppose that a has exponent t, and a' has exponent t', and that t and t' are not co-prime. Then, if t and t' contain no prime factor raised to the same power in both, the exponent of aa' is the L.C.M. of t and t'.

Example.—The exponent of 35 for mod $9 + 6i$ is 6.

The residues of its powers are 35. 16. 14. 22. 29. 1.

The exponent of $3 + 7i$ for the same modulus is 4.

The residues of its powers are $3 + 7i$. 14. $15 + 2i$. 1.

Hence the exponent of $35\,(3 + 7i)$ is the L.C.M. of 6 and $4 = 12$.

$$35\,(3 + 7i) = 105 + 245i \equiv 33 + 2i \pmod{9 + 6i}.$$

The residues of its powers are

$33 + 2i$	29	$33 + i$	22	$2i$	14.
$12 + i$	16	$15 + 2i$	35	$18 + i$	1.

(vii.) The proof is the same as for (7).

If a has exponent t, a' has exponent t', a'' has exponent t'', &c. for modulus m, and if of the $tt't'' \ldots$ numbers $a^r a'^{r'} a''^{r''} \ldots$ (modulus m), formed by giving to r all values modulus t, to r' all values modulus t', &c., no two are congruent; then if

$$a^s a'^{s'} \ldots \equiv 1 \pmod{m},$$

we must have

$$a^s \equiv 1, \; a'^{s'} \equiv 1, \ldots$$

in other words, if a product of powers of numbers that are independent generators be congruent to unity, then each of these powers is itself congruent to unity.

(viii.) Proof identical with (8).

The exponent of the product of a number of independent generators is the L.C.M. of their exponents.

In particular if the separate exponents are all powers of the same prime, then the exponent is equal to the greatest of them.

(ix.) Proof the same as for (9).

If the exponent of a for modulus m is t, and for modulus n is t', and m and n are co-prime, then the exponent of a for modulus mn is the L.C.M. of t and t'.

Also the corollary, if the exponents of a for moduli $m, m', m'', \ldots$ are respectively $t, t', t'', \ldots$ $m, m', m'' \ldots$ being co-prime, then the exponent of a for modulus $mm'm'' \ldots$ is the L.C.M. of the numbers $t, t', t' \ldots$

Example.

$$1 + i \equiv 4 \pmod{2 + i},$$

and the residues of its powers are 4. 1. Hence the exponent of $1 + i$ for modulus $2 + i$ is 2.

$$1 + 1 \equiv 6 \pmod{3 + 2i},$$

and the residues of its powers are 6. 10. 8. 9. 2. 12. 7. 3. 5. 4. 11. 1. Hence the exponent of $1 + i$ for modulus $3 + 2i$ is 12.

The moduli $2 + i$, $3 + 2i$ are co-prime, therefore the exponent of $1 + i$ for modulus $(2 + i)(3 + 2i)$ is 12.

$$1 + i \equiv 19 \pmod{4 + 7i},$$

and the residues of its powers are

19. 36. 34. 61. 54. 51. 59. 16. 44. 56. 24. 1.

Example.

$1 + 2i$ has exp 8, mod 3;

the residues of its powers are

$1 + 2i.\ i.\ 1 + i.\ 2.\ 2 + i.\ 2i.\ 2 + 2i.\ 1.$

$1 + 2i \equiv 11 \pmod{3 + 2i}$, and has exp 12;

the residues of its powers are

11. 4. 5. 3. 7. 12. 2. 9. 8. 10. 6. 1.

$1 + 2i \equiv 26 \pmod{6 + 1}$, and has exp 3,

the residues of its powers are

26. 10. 1.

Hence, since 3, $3 + 2i$, $6 + i$ are co-prime, $1 + 2i$ has for modulus $3(3 + 2i)(6 + i)$ exponent = L.C.M. of 8, 12, 3, *i.e.*, $1 + 2i$ has exponent 24 for modulus $48 + 45i$. The residues of its powers are

$$1 + 2i.\ 90 + i.\ 1339 + i.\ 692.\ 275 + i.\ 1419 + 2i.\ 1370 + 2i.$$
$$1231.\ 1012 + 2i.\ 291 + i.\ 1015 + i.\ 482.$$

$$32 + i.\ 540 + 2i.\ 827 + 2i.\ 211.\ 244 + 2i.\ 969 + i.\ 439 + i.$$
$$269.\ 1043 + i.\ 741 + 2i.\ 503 + 2i.\quad 1.$$

(x.) Proof identical with (10).

If the exponent of a is t, and $t = pqr \ldots$ where $p, q, r \ldots$ are co-prime factors of t, then a can be expressed as a product of numbers whose exponents are $p, q, r \ldots$

Example.—$2 + i$ has exponent 24 for modulus 9. (See example Proposition iv.)

$$24 = 3.\ 8 \qquad \left.\begin{array}{r} 16 \equiv 1 \pmod 3 \\ \equiv 0 \pmod 8 \end{array}\right\} \quad \begin{array}{r} 9 \equiv 1 \pmod 8. \\ \equiv 0 \pmod 3. \end{array}$$

Hence

$$\begin{aligned} 2 + i &\equiv (2 + i)^{16}.\ (2 + i)^9 \pmod 9, \\ &\equiv (7 + 3i)\ (2 + 7i) \pmod 9, \end{aligned}$$

where

and

$$\left.\begin{array}{l} 7 + 3i \text{ has exp } 3 \\ 2 + 7i \text{ has exp } 8 \end{array}\right\} \quad \text{(See example Proposition iv.)}$$

Example.—$33 + 2i$ has exponent 12 for modulus $9 + 6i$. (See example Proposition vi.)

$$12 = 3.\ 4 \qquad \begin{array}{r} 4 \equiv 1 \pmod 3 \\ \equiv 0 \pmod 4 \end{array} \qquad \begin{array}{r} 9 \equiv 1 \pmod 4 \\ \equiv 0 \pmod 3. \end{array}$$

Therefore

$$\begin{aligned} 33 + 2i &\equiv (33 + 2i)^4\ (33 + 2i)^9 \pmod{9 + 6i} \\ &\equiv 22\ (15 + 2i) \pmod{9 + 6i}, \end{aligned}$$

where 22 has exponent 3, and $15 + 2i$ has exponent 4.

(xi.) The number of numbers with exponent t, when the modulus is a prime (pure or mixed), is $\phi(t)$.

Any exponent t is a divisor of $\Phi(p)$, p being the prime modulus (Corollary, Proposition iii.). Exactly as in (11) we see that if there be *one* number with exponent t there are $\phi(t)$ and no more.

Now $t_1, t_2, \ldots$ being all the divisors of any real number $\Phi(p)$,

$$\phi(t_1) + \phi(t_2) + \ldots = \Phi(p).$$

Corresponding to each value t there are $\phi(t)$ numbers, or none with t as exponent.

The number of residues altogether (prime to the modulus p) is $\Phi(p)$. Hence, in no case can there fail to be $\phi(t)$ numbers with exponent t, t being any divisor of $\Phi(p)$.

Corollary.—In particular, any prime modulus p has numbers with exponents $\Phi(p)$, *i.e., has primitive roots.*

The number of these primitive roots is $\phi[\Phi(p)]$.

If p is a pure prime this is $\phi(p^2 - 1)$.

If p is a mixed prime, $= \alpha + \beta i$, the number is $\phi(\alpha^2 + \beta^2 - 1)$.

Example.—Modulus $5 + 2i$. 10 is a primitive root with exponent

$$\Phi(5 + 2i) = (5^2 + 2^2 - 1) = 28.$$

The residues of its powers are given in the table.

Number	10	13	14	24	8	22	17	25	18	6	2	20	26	28
Index	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Number	19	16	15	5	21	7	12	4	11	23	27	9	3	1
Index	15	16	17	18	19	20	21	22	23	24	25	26	27	28 or 0

The $\phi(28) = 12$ primitive roots are 10 14 8 18 2 26 19 15 21 11 27 3.

Example.—Modulus 7. Primitive roots have exponent $\Phi(7) = 7^2 - 1 = 48$. $2 + i$ is a primitive root, and the residues of its powers are given in the table.

Number	$2 + i$	$3 + 4i$	$2 + 4i$	$3i$	$4 + 6i$	$2 + 2i$	$2 + 6i$	5
Index	1	2	3	4	5	6	7	8
Number	$3 + 5i$	$1 + 6i$	$3 + 6i$	i	$6 + 2i$	$3 + 3i$	$3 + 2i$	4
Index	9	10	11	12	13	14	15	16
Number	$1 + 4i$	$5 + 2i$	$1 + 2i$	$5i$	$2 + 3i$	$1 + i$	$1 + 3i$	6
Index	17	18	19	20	21	22	23	24
Number	$5 + 6i$	$4 + 3i$	$5 + 3i$	$4i$	$3 + i$	$5 + 5i$	$5 + i$	2
Index	25	26	27	28	29	30	31	32
Number	$4 + 2i$	$6 + i$	$4 + i$	$6i$	$1 + 5i$	$4 + 4i$	$4 + 5i$	3
Index	33	34	35	36	37	38	39	40
Number	$6 + 3i$	$2 + 5i$	$6 + 5i$	$2i$	$5 + 4i$	$6 + 6i$	$6 + 4i$	1
Index	41	42	43	44	45	46	47	0

The $\phi(48) = 16$ primitive roots are

$$\begin{array}{cccc}
2 + i & 4 + 6i & 2 + 6i & 3 + 6i \\
6 + 2i & 1 + 4i & 1 + 2i & 1 + 3i \\
5 + 6i & 3 + i & 5 + i & 4 + i \\
1 + 5i & 6 + 3i & 6 + 5i & 6 + 4i
\end{array}$$

(xii.) The exponents to which a number a belongs for successive powers of a prime as moduli.

If we make one slight alteration the proof of (12) holds good throughout in the case of complex numbers for powers of a *pure* prime p as moduli. [In place of "$x < p$" read "$x =$ one of the $p^2 - 1$ residues, mod p."]

The exponent of a for mod p^λ is

$$t \text{ if } \lambda \leqq s,$$
$$tp^{\lambda - s} \text{ if } \lambda > s,$$

where t is the exponent of a for mod p, and p^s is the greatest power of p that divides $a^t - 1$.

Corollary.—The greatest value of t is $p^2 - 1$. (Proposition xi.)

The greatest value that $p^{\lambda - s}$ can have is got by making $s = 1$, *i.e.*, by taking a so that $a^{p^2 - 1} - 1$ (though necessarily divisible by p) is not divisible by p^2.

Hence the greatest exponent that a number can have for mod p^λ is

$$(p^2 - 1)p^{\lambda - 1}.$$

Now $\Phi(p^\lambda) = p^{2\lambda} - p^{2(\lambda - 1)} = (p^2 - 1)p^{2(\lambda - 1)}$, which is $p^{\lambda - 1}$ times the highest exponent.

Hence for a *power* of a pure prime as modulus primitive roots do not exist.

Consider next the case of a mixed prime (not $1 + i$).

Suppose $\alpha + \beta i$ is the prime.

Then, if $(\alpha + \beta i)^\lambda = \mathrm{A} + \mathrm{B}i$, A and B must be co-prime, for otherwise $\mathrm{A} + \mathrm{B}i$ would be divisible by some number other than $\alpha + \beta i$.

Hence the $\mathrm{N}(\alpha + \beta i)^\lambda = (\alpha^2 + \beta^2)^\lambda$ residues can be taken to be the pure numbers

$$0,\ 1,\ 2, \ldots (\alpha^2 + \beta^2)^\lambda - 1.$$

Suppose that a is any one of these numbers.

Then, if we have any congruence of the form

$$a^r \equiv b\,[\text{mod } (\alpha + \beta i)^\lambda],$$
$$a^r - b \equiv 0\,[\text{mod } (\alpha + \beta i)^\lambda],$$

it follows, since $a^r - b$ is a pure number, that

$$a^r - b \equiv 0 \,[\text{mod } (\alpha - \beta i)^\lambda],$$

therefore

$$a^r - b \equiv 0 \,[\text{mod } (\alpha^2 + \beta^2)^\lambda],$$
$$a^r \equiv b \,[\text{mod } (\alpha^2 + \beta^2)^\lambda].$$

Hence for the modulus $(\alpha + \beta i)^\lambda$ the residue of any power of a number is the same as for the modulus $(\alpha^2 + \beta^2)^\lambda$.

Now $\alpha^2 + \beta^2$ is a *real prime.*

Therefore the exponent to which a belongs for modulus $(\alpha + \beta i)^\lambda$ is

$$t \text{ if } \lambda \leqq s,$$
$$t\,(\alpha^2 + \beta^2)^{\lambda - s} \text{ if } \lambda > s,$$

where t is the exponent of a for mod $\alpha^2 + \beta^2$, and $(\alpha^2 + \beta^2)^s$ is the highest power of $\alpha^2 + \beta^2$ that divides $a^t - 1$.

The greatest exponent is

$$(\alpha^2 + \beta^2 - 1)\,(\alpha^2 + \beta^2)^{\lambda - 1},$$

and

$$\Phi\,(\alpha + \beta i)^\lambda = (\alpha^2 + \beta^2)^\lambda - (\alpha^2 + \beta^2)^{\lambda - 1} = (\alpha^2 + \beta^2 - 1)\,(\alpha^2 + \beta^2)^{\lambda - 1}.$$

Thus for powers of a *mixed prime* primitive roots *do* exist.

(xii*a*.) We see from the last proposition that for a power of a mixed prime as modulus primitive roots exist, and any one of them generates by its powers all the residues prime to the modulus. But in the case of a power of a pure prime p^λ, the highest exponent is $p^{\lambda-1}(p^2 - 1)$, whereas $\Phi\,(p^\lambda) = p^{2(\lambda - 1)}(p^2 - 1)$.

We wish now to find how all the $p^{2(\lambda-1)}(p^2 - 1)$ numbers can be generated.

$$\left.\begin{array}{l}\text{Take a number } g \text{ with exp } p^{\lambda-1}(p^2 - 1) \\ \text{and ,, } \quad \text{,, } \quad f \quad \text{,, } \quad \text{,, } \quad p^{\lambda-1}\end{array}\right\}$$

g can be expressed as a product

$$g \equiv f'h \;(\text{mod } p^\lambda),$$

where

$$\left.\begin{array}{l}f' \text{ has exp } p^{\lambda-1} \\ h \quad \text{,, } \quad \text{,, } \quad p^{2} - 1\end{array}\right\}, \text{ Proposition x.}$$

$$\left.\begin{array}{r}f \text{ and } f' \text{ are each} \equiv 1 \;(\text{mod } p) \\ \not\equiv 1 \;(\text{mod } p^2)\end{array}\right\}, \text{ Proposition xii.}$$

Suppose

$$f \equiv 1 + \alpha p \pmod{p^2} \qquad \alpha \not\equiv 0 \pmod{p},$$
$$f' \equiv 1 + \alpha' p \pmod{p^2} \qquad \alpha' \not\equiv 0 \pmod{p}.$$

The $p^{\lambda-1} \times p^{\lambda-1} (p^2 - 1)$ numbers generated by products of powers of f and g will be the $p^{2(\lambda-1)} (p^2 - 1)$ residues prime to the modulus p^λ, provided that no two of them are congruent. We shall now show that no two can be congruent provided that k is a *complex* and not a *real* number, k being determined by the congruence $k\alpha' \equiv \alpha \pmod{p}$.

Suppose that two of the numbers generated are congruent, say

$$g^i f^j \equiv g^{i'} f^{j'} \pmod{p^\lambda},$$

where

$$i \not\equiv i' \pmod{p^{\lambda-1} \,.\, p^2 - 1},$$
$$j \not\equiv j' \pmod{p^{\lambda-1}}.$$

This is equivalent to

$$g^{i''} \equiv f^{j''} \pmod{p^\lambda},$$

where

$$i'' \equiv i - i' \not\equiv 0 \pmod{p^{\lambda-1} \,.\, p^2 - 1},$$
$$j'' \equiv j - j' \not\equiv 0 \pmod{p^{\lambda-1}},$$

j'' may be divisible by a power of p.

Suppose

$$j'' = \beta p^{\lambda-s},$$

where β is prime to p, and s may be any one of the numbers 2, 3, . . . λ.

Then

$$f^{j''} \text{ has exp } p^{s-1}. \quad \text{(Proposition iv.)},$$

therefore

$$g^{i''} \text{ has exp } p^{s-1},$$

therefore

$$i'' = \beta' (p^2 - 1) p^{\lambda-s},$$

where β' is prime to p. (Proposition iv.) Therefore

$$g^{\beta'(p^2-1)p^{\lambda-s}} \equiv f^{\beta p^{\lambda-s}} \pmod{p^\lambda},$$

and, therefore, since

$$h^{p^2-1} \equiv 1 \pmod{p^\lambda},$$
$$f'^{\beta'(p^2-1)p^{\lambda-s}} \equiv f^{\beta p^{\lambda-s}} \pmod{p^\lambda}.$$

Raise both sides to the power p^{s-2}, then

$$f'^{\beta'(p^2-1)p^{\lambda-2}} \equiv f^{\beta p^{\lambda-2}} \pmod{p^\lambda}.$$

Let

$$\beta\xi \equiv 1 \pmod{p}$$

determine ξ, and suppose

$$\beta' (p^2 - 1)\, \xi \equiv \gamma \pmod{p}.$$

Raise both sides to the power ξ, then

$$f'^{\gamma p^{\lambda-2}} \equiv f^{p^{\lambda-2}} \pmod{p^\lambda}.$$

Now

$$f \equiv 1 + \alpha p \pmod{p^2},$$

therefore

$$f^{p^{\lambda-2}} \equiv 1 + \alpha p^{\lambda-1} \pmod{p^\lambda},$$

and

$$f' \equiv 1 + \alpha' p \pmod{p^2},$$

therefore

$$f'^{\gamma p^{\lambda-2}} \equiv 1 + \alpha' \gamma p^{\lambda-1} \pmod{p^\lambda},$$

therefore

$$1 + \alpha' \gamma p^{\lambda-1} \equiv 1 + \alpha p^{\lambda-1} \pmod{p^\lambda},$$

therefore

$$\gamma\alpha' \equiv \alpha \pmod{p},$$

therefore

$$\gamma \equiv k \pmod{p}.$$

Now i'', j'', β, β', and, therefore, ξ, and finally γ, are *real* numbers, whereas, by supposition, k is complex, therefore on this supposition g and f are complete generators.

Example.—Modulus 3^2.

$$\Phi(3^2) = 3^4 - 3^2 = 72.$$

The highest exponent is

$$3(3^2 - 1) = 24.$$

We shall find that $2 + i$ and $4 + 3i$ can be taken for generators.

$$\left.\begin{aligned} g &= 2 + i \text{ has exp } 24 \text{ mod } 3^2 \\ f &= 4 + 3i \text{ has exp } \ \ 3 \text{ mod } 3^2 \end{aligned}\right\}$$

$$\begin{aligned} 2 + i &\equiv (2 + i)^{16} (2 + i)^9 \pmod{9} \\ &\equiv (7 + 3i)(2 + 7i) \pmod{9}, \end{aligned}$$

and

$$f' = 7 + 3i \text{ has exp } 3.$$

Now

$$f \equiv 1 + (1 + i) \,.\, 3 \pmod{3^2}$$
$$f' \equiv 1 + (2 + i) \,.\, 3 \pmod{3^2}$$

and

$$k(2+i) \equiv (1+i) \pmod{3}$$

gives

$$k \equiv 2i,$$

which is not a real number.

The following table gives the indices of the 72 numbers.

	0	1	2
1	$2+i$	$5+i$	$8+i$
2	$3+4i$	$7i$	$6+i$
3	$2+2i$	$2+5i$	$2+8i$
4	$2+6i$	$8+3i$	5
5	$7+5i$	$4+5i$	$1+5i$
6	$8i$	$3+5i$	$6+2i$
7	$1+7i$	$1+4i$	$1+i$
8	$4+6i$	7	$1+3i$
9	$2+7i$	$5+7i$	$8+7i$
10	$6+7i$	$3+i$	$4i$
11	$5+2i$	$5+5i$	$5+8i$
12	8	$5+6i$	$2+3i$
13	$7+8i$	$4+8i$	$1+8i$
14	$6+5i$	$2i$	$3+8i$
15	$7+7i$	$7+4i$	$7+i$
16	$7+3i$	$1+6i$	4
17	$2+4i$	$5+4i$	$8+4i$
18	i	$6+4i$	$3+7i$
19	$8+2i$	$8+5i$	$8+8i$
20	$5+3i$	2	$8+6i$
21	$7+2i$	$4+2i$	$1+2i$
22	$3+2i$	$6+8i$	$5i$
23	$4+7i$	$4+4i$	$4+i$
0	1	$4+3i$	$7+6i$

[The pair of indices for any number are found at the end of the row and at the head of the column in which the number is situated.

Thus

$$1+8i \equiv (2+i)^{13}(4+3i)^{2} \pmod{9}.]$$

(xiii.–xvi.) Propositions (13) to (16) are concerned with the moduli 2^λ. In Propositions xiii.–xvi. we shall investigate the moduli analogous to these in the case of complex numbers, viz. $(1+i)^\lambda$. [Propositions xiii.–xvi. will not be made to correspond individually to Propositions (13)–(16): they are intended to cover the same ground.]

(xiii.) In the case of the smaller values of λ, from 1 to 7, we shall find results, some of which, though they are really particular cases of the general results for any value of λ, are not conveniently included under them.

We shall start by a separate treatment of each of the first seven moduli, finding—

(i.) the numbers which belong to each exponent;
(ii.) what numbers must be taken in order to generate the complete set of residues.

Mod $1+i$. There is only one residue, viz., 1, whose exponent is 1.

Mod $(1+i)^2$. $\Phi(1+i)^2 = 2$. There are two numbers, viz.,

$$\left.\begin{matrix} i \text{ with exp } 2 \\ \text{and} \quad 1 \text{ with exp } 1 \end{matrix}\right\}.$$

Thus, for this modulus, i is a primitive root.

Mod $(1+i)^3$. $\Phi(1+i)^3 = 4$. The four residues are—

$$\begin{aligned} i,\ 2+i &\text{ with exp } 4, \\ 3 &\text{ with exp } 2, \\ 1 &\text{ with exp } 1. \end{aligned}$$

i and $2+i$ are both primitive roots.

Mod $(1+i)^4$. $\Phi(1+i)^4 = 8$. The 8 numbers with their exponents are

Exp 4.	i,	$3i$,	$2+i$,	$2+3i$.
Exp 2.	3,	$1+2i$,	$3+2i$.	
Exp 1.	1.			

The square of each of the four numbers with exponent 4 is congruent to the same number with exponent 2, viz. 3.

Hence, to generate the 8 numbers, we must take any one of the four numbers with exponent 4, and either of the two numbers with exponent 2, viz. $1+2i$, $3+2i$.

Mod $(1+i)^5$. $\Phi(1+i)^5 = 16$. The 16 numbers, with their exponents are

Exp 4.	i	$3i$	$2+i$	$2+3i$	$4+i$	$6+i$	$4+3i$	$6+3i$.
Exp 2.	3	5	7	$1+2i$	$3+2i$	$5+2i$	$7+2i$	
Exp 1.	1.							

The square of each of the 8 numbers with exponent 4 gives the same number with exponent 2, viz. 7.

Also $7 \equiv 3 \,.\, 5 \equiv (1 + 2i)(3 + 2i) \equiv (5 + 2i)(7 + 2i) \,.\, [\text{mod } (1 + i)^5]$.

Hence, firstly, we must take as generators

and $$\left.\begin{array}{l}\text{one number with exponent 4}\\ \text{two numbers with exponent 2}\end{array}\right\};$$

and, secondly, the two numbers with exponent 2 must neither of them be 7, and they must not be a pair of the numbers as arranged above whose product is congruent to 7.

Mod $(1 + i)^6$. $\Phi(1 + i)^6 = 32$. The 32 numbers with their exponents are arranged below.

Exp 1.	Exp 2.	Exp 4.							
1	$5+4i$	$1+2i$	$1+6i$	$3+2i$	$3+6i$	$5+2i$	$5+6i$	$7+2i$	$7+6i$
	$3+4i$	$2+i$	$2+3i$	$2+5i$	$2+7i$	$6+i$	$6+3i$	$6+5i$	$6+7i$
	7	$4+i$	$4+3i$	$4+5i$	$4+7i$	i	$3i$	$5i$	$7i$
	3								
	5								
	$1+4i$								
	$7+4i$								

The 24 numbers with exponent 4 are written in three rows, and the number with exponent 2, to which the square of any one of them is congruent, is to be found written at the end of the row.

Moreover, the three numbers, with exponent 2 (viz. $5 + 4i$, $3 + 4i$ and 7), which thus appear as the squares of numbers with exponent 4, are such that the product of any two is congruent to the third; for

$$7(5 + 4i)(3 + 4i) \equiv 1 \; [\text{mod } (1 + i)^6].$$

Hence, to generate the 32 numbers, we must take

two numbers, with exponent 4, not in the same row

and

one number, with exponent 2, selected from 3, 5, $1 + 4i$, $7 + 4i$.

Mod $(1+i)^7$. $\Phi(1+i)^7 = 64$. The 64 numbers, with their exponents, are arranged below.

Exp 1.	*Exp* 2.	*Exp* 4.							
1	7	$4+i$	$12+i$	$3i$	$8+3i$	$5i$	$8+5i$	$4+7i$	$12+7i$
	9	3	5	11	13	$1+4i$	$7+4i$	$9+4i$	$15+4i$
	15	i	$8+i$	$4+3i$	$12+3i$	$4+5i$	$12+5i$	$7i$	$8+7i$
	$3+4i$	$2+i$	$10+i$	$2+3i$	$10+3i$	$6+5i$	$14+5i$	$6+7i$	$14+7i$
	$5+4i$	$5+2i$	$7+2i$	$13+2i$	$15+2i$	$1+6i$	$3+6i$	$9+6i$	$11+6i$
	$11+4i$	$6+i$	$14+i$	$6+3i$	$14+3i$	$2+5i$	$10+5i$	$2+7i$	$10+7i$
	$13+4i$	$1+2i$	$3+2i$	$9+2i$	$11+2i$	$5+6i$	$7+6i$	$13+6i$	$15+6i$

The 56 numbers with exponent 4 are arranged in rows collinearly with the numbers, with exponent 2, to which their squares are congruent.

The 7 numbers with exponent 2 can be arranged in 7 sets of 3, so that of each 3 the product of any two is congruent to the third (or the product of the three congruent to unity). Thus:

$$\left.\begin{array}{r} 7.\ 9.\ 15 \equiv 1 \\ 7\,(13+4i)\,(3+4i) \equiv 1 \\ 7\,(5+4i)\,(11+4i) \equiv 1 \\ 9\,(3+4i)\,(11+4i) \equiv 1 \\ 9\,(5+4i)\,(13+4i) \equiv 1 \\ 15\,(3+4i)\,(5+4i) \equiv 1 \\ 15\,(11+4i)\,(13+4i) \equiv 1 \end{array}\right\} (\text{mod } 1+i)^7.$$

To generate the 64 numbers, we must take three numbers each with exponent 4. The product of powers of three such numbers can only be congruent to unity without each being separately congruent to unity, if the product of their squares be so.

Hence, the three generators must be chosen, one each from three of the above rows, and the numbers, with exponent 2 found in these rows, must not have their product congruent to unity.

(xiv.) *The numbers which have as exponents* 2, 4, *and* 8 *for mod* $(1+i)^\lambda$.

We shall use the results of the three following Lemmas:

Lemma (1).—If

$$a^2 \equiv 1 \ [\text{mod } (1+i)^\kappa]$$

$$(a-1)\,(a+1) \equiv 0 \ [\text{mod } (1+i)^\kappa]$$

Now, if

$$a \equiv 1 \ [\text{mod } (1+i)^3]$$

$$a + 1 \equiv 2 \ [\text{mod } (1+i)^3]$$

$$\equiv 0 \ [\text{mod } (1+i)^2],$$

i.e., if $a - 1$ is divisible by $(1 + i)^3$ or any higher power, then $a + 1$ is divisible by $(1 + i)^2$ as the highest power.

Similarly, we can show that if a higher power than $(1 + i)^2$ divides $a + 1$, then no higher power than $(1 + i)^2$ divides $a - 1$.

Therefore, if $\kappa > 4$, either

$$a \equiv 1 \; [\bmod\, (1 + i)^{\kappa - 2}]$$

or

$$a \equiv - 1 \; [\bmod\, (1 + i)^{\kappa - 2}],$$

therefore, κ being > 4, the solutions of

$$a^2 \equiv 1 \; [\bmod\, (1 + i)^{\kappa}]$$

are given by

$$a \equiv \pm 1 \; [\bmod\, (1 + i)^{\kappa - 2}].$$

Lemma (2).—If

$$a^2 \equiv - 1 \; [\bmod\, (1 + i)^{\kappa}]$$

$$(a + i)\,(a - i) \equiv 0 \; [\bmod\, (1 + i)^{\kappa}]$$

Now, if

$$a \equiv i \; [\bmod\, (1 + i)^{3}]$$

$$a + i \equiv 2i \; [\bmod\, (1 + i)^{3}]$$

$$\equiv 0 \; [\bmod\, (1 + i)^{2}].$$

Thus as above, if either of $a + i$, $a - i$ is divisible by a power of $(1 + i)$ above the second, then $(1 + i)^2$, is the highest power that divides the other.

Therefore, if $\kappa > 4$ the solutions of

$$a^2 \equiv - 1 \; [\bmod\, (1 + i)^{\kappa}]$$

are given by

$$a \equiv \pm i \; [\bmod\, (1 + i)^{\kappa - 2}].$$

Lemma (3).

$$a^2 \equiv \pm i \; [\bmod\, (1 + i)^{\kappa}]$$

is impossible for any value of $\kappa > 1$.

For if so,

$$a^2 \equiv \pm i \; [\bmod\, (1 + i)^{2}],$$

or

$$a^2 \equiv i \; [\bmod\, (1 + i)^{2}],$$

since

$$- i \equiv i \; [\bmod\, (1 + i)^{2}],$$

which is impossible, for

$$1^2 \not\equiv i \; [\bmod\, (1 + i)^{2}],$$

and

$$\iota^2 \not\equiv i \; [\bmod\, (1 + i)^{2}].$$

Numbers with exponent 2 *mod* $(1 + i)^\lambda$. $(\lambda > 4.)$

All these numbers, together with 1, which has exponent 1, satisfy the congruence

$$a^2 \equiv 1 \,[\text{mod } (1 + i)^\lambda];$$

therefore

$$a \equiv \pm 1 \,[\text{mod } (1 + i)^{\lambda - 2}]$$

gives (together with unity) the numbers which have exponent 2, mod $(1 + i)^\lambda$.

We get thus 7 numbers with exponent 2, mod $(1 + i)^\lambda$. They are congruent to

$$\left.\begin{array}{l} -1 \\ \pm 1 + (1 + i)^{\lambda - 2} \\ \pm 1 + (1 + i)^{\lambda - 1} \\ \pm 1 + (1 + \iota)^{\lambda - 2} + (1 + i)^{\lambda - 1} \end{array}\right\} [\text{mod } (1 + i)^\lambda].$$

The product of any two of these is congruent to a third. If we name the 7 numbers thus—

$$\begin{aligned} \alpha &\equiv - 1, \\ \beta &\equiv + 1 + (1 + i)^{\lambda - 2}, \\ \gamma &\equiv - 1 + (1 + i)^{\lambda - 2}, \\ \delta &\equiv + 1 + (1 + i)^{\lambda - 1}, \\ \epsilon &\equiv - 1 + (1 + i)^{\lambda - 1}, \\ \eta &\equiv + 1 + (1 + i)^{\lambda - 2} + (1 + i)^{\lambda - 1}, \\ \theta &\equiv - 1 + (1 + i)^{\lambda - 2} + (1 + i)^{\lambda - 1}, \end{aligned}$$

then these relations may be written thus—

$$\begin{aligned} \alpha\beta\gamma &\equiv 1, \\ \alpha\delta\epsilon &\equiv 1, \\ \alpha\eta\theta &\equiv 1, \\ \beta\delta\eta &\equiv 1 \\ \beta\epsilon\theta &\equiv 1, \\ \gamma\delta\theta &\equiv 1, \\ \gamma\epsilon\eta &\equiv 1, \end{aligned}$$

[which includes $\alpha\beta \equiv \gamma$, $\alpha\gamma \equiv \beta$, $\beta\gamma \equiv \alpha$, because $\alpha^2 \equiv 1$, $\beta^2 \equiv 1$, $\gamma^2 \equiv 1$].

Numbers with exponent 4, *mod* $(1 + i)^\lambda$. $(\lambda > 6.)$

The numbers which satisfy

$$a^4 \equiv 1 \,[\text{mod}\,(1 + i)^\lambda],$$

and which do not satisfy

$$a^2 \equiv 1 \,[\text{mod } (1+i)^{\lambda}],$$

are the numbers with exponent 4.

Hence Lemma (1) gives us

$$a^2 \equiv \pm 1 \,[\text{mod } (1+i)^{\lambda-2}],$$

and then Lemma (2) gives

$$a \equiv \pm 1, \ \pm i \,[\text{mod } (1+i)^{\lambda-4}].$$

If of these numbers we exclude

$$a \equiv \pm 1 \,[\text{mod } (1+i)^{\lambda-2}],$$

we have the numbers with exponent 4.

Hence the numbers with exponent 4 are

$$\equiv \pm i \,[\text{mod } (1+i)^{\lambda-4}],$$

and

$$\left.\begin{aligned} &\equiv \pm 1 + (1+i)^{\lambda-4} \\ &\quad \pm 1 + (1+i)^{\lambda-3} \\ &\quad \pm 1 + (1+i)^{\lambda-4} + (1+i)^{\lambda-3} \end{aligned}\right\} \text{mod } (1+i)^{\lambda-2}.$$

The number of these is

$$\begin{aligned} &2\text{N}\,[(1+i)^4] + 6\text{N}\,[(1+i)^2] \\ &= 2 \,.\, 2^4 + 2 \,.\, 3 \,.\, 2^2 \\ &= 2^5 + 3 \,.\, 2^3 \\ &= 2^5 + 2^4 + 2^3 = 56. \end{aligned}$$

Numbers with exponent 8 *mod* $(1+i)^{\lambda}$. $\lambda > 8$.

The numbers are those that satisfy

$$a^8 \equiv 1 \,[\text{mod } (1+i)^{\lambda}],$$

excluding those that satisfy

$$a^4 \equiv 1 \,[\text{mod } (1+i)^{\lambda}].$$

Now

$$a^8 \equiv 1 \,[\text{mod } (1+i)^{\lambda}]$$

gives

$$a^4 \equiv \pm 1 \,[\text{mod } (1+i)^{\lambda-2}]. \quad \text{Lemma (1).}$$

$$a^2 \equiv \pm 1 \,[\text{mod } (1+i)^{\lambda-4}]. \quad \text{Lemmas (1), (2), and (3)}$$

$$a \equiv \pm 1, \ \pm i \,[\text{mod } (1+i)^{\lambda-6}]. \quad \text{Lemmas (1) and (2)}$$

Of these we have to exclude

$$a \equiv \pm 1 \ \pm i, \,[\text{mod } (1+i)^{\lambda-4}].$$

Hence the numbers with exponent 8 are

$$\left.\begin{array}{l}\pm 1,\ \pm i,\ +(1+i)^{\lambda-6}\\ \pm 1,\ \pm i,\ +(1+i)^{\lambda-5}\\ \pm 1,\ \pm i,\ +(1+i)^{\lambda-6}+(1+i)^{\lambda-5}\end{array}\right\}\bmod (1+i)^{\lambda-4}.$$

In number they are

$$\begin{aligned} &4 \times 3 \times \mathrm{N}(1+i)^4\\ &= 2^2 . 3 . 2^4\\ &= 2^6 + 2^7.\end{aligned}$$

We have not specially examined the modulus $(1+i)^8$. The general results already obtained give us the numbers with exponents 2 and 4. We will find the numbers with exponent 8.

Of the solutions of

$$a^8 \equiv 1\,[\bmod (1+i)^8]$$

we must exclude those of

$$a^4 \equiv 1\,[\bmod (1+i)^8].$$

$$a^8 \equiv 1\,[\bmod (1+i)^8]$$

gives

$$a^4 \equiv \pm 1\,[\bmod (1+i)^6]$$

and

$$a^2 \equiv \pm 1\,[\bmod (1+i)^4],$$

and therefore

$$a \equiv i,\ 3i,\ 2+i,\ 2+3i,\ 3,\ 1+2i,\ 3+2i,\ 1\,[\bmod (1+i)^4].\quad [\text{See mod } (1+i)^4.]$$

The numbers to be excluded are

$$\begin{aligned} a^4 &\equiv 1\,[\bmod (1+i)^8]\\ a^2 &\equiv \pm 1\,[\bmod (1+i)^6]\\ a &\equiv \pm 1,\ \pm i\,[\bmod (1+i)^4],\end{aligned}$$

i.e.,

$$a \equiv 1,\ 3,\ i,\ 3i\,[\bmod (1+i)^4].$$

Hence the numbers $\equiv 2+i,\ 1+2i,\ 2+3i,\ 3+2i\,[\bmod (1+i)^4]$ have exponent 8. The number of them is $4 \times 2^4 = 2^6$.

(xv.) *The numbers which have exponent* 2^s *for mod* $(1+i)^\lambda$. [$\lambda > 8$ and $s > 3$.] The numbers are those which satisfy

$$a^{2^s} \equiv 1 \; [\text{mod } (1+i)^\lambda],$$

and which do not satisfy

$$a^{2^{s-1}} \equiv 1 \; [\text{mod } (1+i)^\lambda].$$

The first gives

$$a \equiv \pm 1, \; \pm i \; [\text{mod } (1+i)^{\lambda-2s}] \text{ if } \lambda - 2s > 2,$$

and the second

$$a \equiv \pm 1, \; \pm i, \; [\text{mod } (1+i)^{\lambda-2s+2}].$$

Hence the numbers with exponent 2^s for mod $(1+i)^\lambda$, $(\lambda - 2s > 2)$, are

$$\left.\begin{array}{l} \pm 1, \; \pm i, \; + (1+i)^{\lambda-2s} \\ \pm 1, \; \pm i, \; + (1+i)^{\lambda-2s+1} \\ \pm 1, \; \pm i, \; + (1+i)^{\lambda-2s} + (1+i)^{\lambda-2s+1} \end{array}\right\} \text{mod } (1+i)^{\lambda-2s+2}.$$

The number of them is

$$\begin{aligned} & 12 \times \mathrm{N}\,(1+i)^{2s-2} \\ & = 2^2.\ 3.\ 2^{2s-2} \\ & = 2^{2s} + 2^{2s+1}. \end{aligned}$$

If λ is odd, $= 2\mu + 1$ the greatest value of s is $\mu - 1$, and then $\lambda - 2s > 2$. So there are $2^{2\mu-2} + 2^{2\mu-1}$ numbers with exponent $2^{\mu-1}$ for mod $(1+i)^{2\mu+1}$, viz.,

$$\left.\begin{array}{l} \pm 1, \pm i, + (1+i)^3 \\ \pm 1, \pm i, + (1+i)^4 \\ \pm 1, \pm i, + (1+i)^3 + (1+i)^4 \end{array}\right\} \text{mod } (1+i)^5,$$

$$\equiv \left.\begin{array}{cccc} 7+2i, & 5+2i, & 6+3i, & 6+i \\ 5 & 3 & 4+i & 3i \\ 3+2i, & 1+2i, & 2+3i, & 2+i \end{array}\right\} \text{mod } (1+i)^5.$$

So for mod $(1+i)^{2\mu+1}$ there are

$$\left.\begin{array}{llll} 2^{2\mu-1} + 2^{2\mu-2} & \text{numbers with exp} & & 2^{\mu-1} \\ \cdots & \cdots & \cdots & \cdots \\ 2^{2s+1} + 2^{2s} & \text{,,} \quad \text{,,} & \text{,,} & 2^s \\ \cdots & \cdots & \cdots & \cdots \\ 2^7 + 2^6 & \text{,,} \quad \text{,,} & \text{,,} & 2^3 \\ 2^5 + 2^4 + 2^3 & \text{,,} \quad \text{,,} & \text{,,} & 2^2 \\ 2^2 + 2 + 1 & \text{,,} \quad \text{,,} & \text{,,} & 2 \\ 1 & \text{,,} \quad \text{,,} & \text{,,} & 1 \end{array}\right\}$$

making, in all, $2^{2\mu} = \Phi\,(1+i)^{2\mu+1}$ numbers, as it should.

If λ is even and $= 2\mu$, then we may have $s = \mu + 1$, and in this case $\lambda - 2s = 2$. We wish, therefore, to find the numbers with exponent $2^{\mu-1}$ for mod $(1 + i)^{2\mu}$.

We have to take the solutions of

$$a^{2^{\mu-1}} \equiv 1 \; [\text{mod } (1 + i)^{2\mu}]$$

and exclude those of

$$a^{2^{\mu-2}} \equiv 1 \; [\text{mod } (1 + i)^{2\mu}].$$

The first leads to

$$a^2 \equiv \pm 1 \; [\text{mod } (1 + i)^4],$$

and the second to

$$a \equiv \pm 1, \; \pm i \; [\text{mod } (1 + i)^4],$$

therefore

$$a \equiv 1 + 2i, \; 2 + i, \; 3 + 2i, \; 2 + 3i \; [\text{mod } (1 + i)^4].$$

Hence the numbers with exponent $2^{\mu-1}$ for mod $(1 + i)^{2\mu}$ are

$$\equiv 1 + 2i, \; 2 + i, \; 3 + 2i, \; 2 + 3i \; [\text{mod } (1 + i)^4].$$

The number of them is $4 \times \text{N} (1 + i)^{2\mu-4}$

$$= 2^2 . 2^{2\mu-4}$$
$$= 2^{2\mu-2}.$$

For mod $(1 + i)^{2\mu}$ there are

$$\left.\begin{array}{lcccl}
2^{2\mu-2} & \text{numbers} & \text{with} & \text{exp} & 2^{\mu-1} \\
2^{2\mu-3} + 2^{2\mu-4} & ,, & ,, & ,, & 2^{\mu-2} \\
\cdot\;\cdot\;\cdot\;\cdot & \cdot\;\cdot\;\cdot & \cdot\;\cdot\;\cdot & \cdot\;\cdot\;\cdot & \cdot \\
2^{2s+1} + 2^{2s} & ,, & ,, & ,, & 2^{s} \\
\cdot\;\cdot\;\cdot\;\cdot & \cdot\;\cdot\;\cdot & \cdot\;\cdot\;\cdot & \cdot\;\cdot\;\cdot & \cdot \\
2^7 + 2^6 & ,, & ,, & ,, & 2^3 \\
2^5 + 2^4 + 2^3 & ,, & ,, & ,, & 2^2 \\
2^2 + 2 + 1 & ,, & ,, & ,, & 2 \\
1 & ,, & ,, & ,, & 1
\end{array}\right\}$$

making, in all, $2^{2\mu-1} = \Phi \, (1 + i)^{2\mu}$ numbers as it should.

(xvi.) *Generators for the modulus* $(1 + i)^{\lambda}$.

If $\lambda = 2\mu + 1$, it is easy to see that in order to generate $2^{2\mu}$ numbers, of which for each exponent there shall be the right number of numbers (as just found), we must take three generators :—

$$\left.\begin{array}{l}
\text{two generators with exp } 2^{\mu-1} \\
\text{and} \\
\text{one generator with exp } 2^2
\end{array}\right\}.$$

If $\lambda = 2\mu$, we can similarly see that we must take three generators

$$\left.\begin{array}{lll}\text{one generator with exp} & & 2^{\mu-1} \\ \quad ,, & ,, & 2^{\mu-2} \\ \quad ,, & ,, & 2^{2}\end{array}\right\} .$$

We have now to show how these may be selected, so that all the numbers generated may be incongruent.

Any number, with exponent > 2 modulus $(1 + i)^{\lambda}$, has one of its powers, and one only, which has exponent 2.

Suppose all the numbers modulus $(1 + i)^{\lambda}$, arranged in 7 groups, so that all the numbers in a group may have the same number, with exponent 2, as a power.

We shall now prove four Lemmas with regard to these groups.

Lemma (i.). A power of a number belonging to any group belongs to the same group.

Let a have exponent 2^s, and belong to the group α, *i.e.*,

$$a^{2^{s-1}} \equiv \alpha \left[\text{mod } (1 + i)^{\lambda}\right].$$

Take any power of a, say $a^{2^{\sigma}i}$ where i is odd.

Its exponent is $2^{s-\sigma}$. (Proposition iv.)

Therefore

$$(a^{2^{\sigma}i})^{2^{s-\sigma-1}} \text{ has exp } 2,$$

i.e.,

$$a^{2^{s-1}i} \text{ has exp } 2,$$

and it is $\equiv \alpha^i$, and, therefore, $\equiv \alpha$, because i is odd.

Therefore, any power of a belongs to the same group.

Lemma (ii.). If a and a' have exponent 2^s, and belong to the same group α, then

$$(aa')^{2^{s-1}} \equiv 1 \left[\text{mod } (1 + i)^{\lambda}\right].$$

For

$$a^{2^{s-1}} \equiv \alpha.$$

$$a'^{2^{s-1}} \equiv \alpha.$$

Therefore

$$(aa')^{2^{s-1}} \equiv \alpha^2 \equiv 1 \left[\text{mod } (1 + i)^{\lambda}\right].$$

Lemma (iii). If

$$a \text{ has exp } 2^s \text{ and belongs to group } \alpha,$$

and

$$b \quad ,, \quad 2^s \quad ,, \quad ,, \quad \beta,$$

then

$$ab \quad ,, \quad 2^s \quad ,, \quad ,, \quad \gamma,$$

where

$$\alpha\beta\gamma \equiv 1.$$

For

$$a^{2^s-1} \equiv \alpha,$$
$$b^{2^s-1} \equiv \beta.$$

Therefore

$$(ab)^{2^s-1} \equiv \alpha\beta \equiv \gamma \text{ [mod } (1+i)^\lambda],$$

and, therefore,

ab has exp 2^s, and belongs to group γ.

Lemma (iv.). If

a has exp $2^{s+\sigma}$ and belongs to group α,

and

b ,, 2^s ,, ,, β,

then

ab ,, $2^{s+\sigma}$,, ,, α.

For

$$a^{2^{s+\sigma-1}} \equiv \alpha,$$
$$b^{2^s-1} \equiv \beta,$$

and, therefore,

$$b^{2^{s+\sigma-1}} \equiv 1.$$

Therefore

$$(ab)^{2^{s+\sigma-1}} \equiv \alpha.$$

Therefore

ab has exp $2^{s+\sigma}$, and belongs to group α.

Now, suppose that we take these generators with the necessary exponents. They must be chosen so that the numbers they generate are all incongruent.

Let g_1, g_2, g_3 be the generators.

Then, $g_1^{i_1}, g_2^{i_2}, g_3^{i_3} \equiv g_1^{i_1'}, g_2^{i_2'}, g_3^{i_3'}$ [mod $(1+i)^\lambda$] must be impossible unless

$$i_1 \equiv i_1' \text{ (mod exp } g_1),$$
$$i_2 \equiv i_2' \text{ (mod exp } g_2),$$
$$i_3 \equiv i_3' \text{ (mod exp } g_3),$$

i.e., $g_1^{j_1}, g_2^{j_2}, g_3^{j_3} \equiv 1$ [mod $(1+i)^\lambda$] must be possible only when

$$j_1 \equiv 0 \text{ (mod exp } g_1), \quad j_2 \equiv 0 \text{ (mod exp } g_2), \quad j_3 \equiv 0 \text{ (mod exp } g_3).$$

We shall now show that to render this so, the three generators must belong to three different groups, and that those three groups must not be any one of the seven sets of three, such as α, β, γ, for which $\alpha\beta\gamma \equiv 1$.

Let us denote the exponents of g_1, g_2, g_3 by 2^{s_1}, 2^{s_2}, 2^{s_3}. [When λ is odd these are $2^{\mu-1}$, $2^{\mu-1}$, 2^2, and when λ is even, $2^{\mu-1}$, $2^{\mu-2}$, 2^2.]

First suppose that any two of the generators belong to the *same* group.

Say g_1 and g_2 both belong to the same group ; s_1 and s_2 may be equal or unequal.

If $s_1 = s_2$, Lemma (ii.) shows that the exponent of $g_1 g_2$ divides 2^{s_1-1}, therefore

$$(g_1 g_2)^{2^{s_1-1}} \equiv 1 \, [\text{mod } (1+i)^\lambda],$$

$$g_1^{2^{s_1-1}} g_2^{2^{s_2-1}} \equiv 1 \, [\text{mod } (1+i)^\lambda],$$

where

$$2^{s_1-1} \not\equiv 0 \pmod{2^{s_1}},$$

$$2^{s_2-1} \not\equiv 0 \pmod{2^{s_2}},$$

therefore g_1, g_2, cannot belong to the same group.

If $s_1 = s_2 + \sigma$, then $g_2^{2^\sigma}$ has exponent s_1, and Lemma (ii.) shows that

$$g_1^{2^{s_1-1}} g_2^{2^{\sigma+s_1-1}} \equiv 1 \, [\text{mod } (1+i)^\lambda],$$

where

$$2^{s_1-1} \equiv 0 \, [\text{mod } (1+i)^\lambda],$$

therefore g_1 and g_2 cannot belong to the same group.

Hence the three generators must belong to three different groups.

Next suppose that the three generators belong to three groups, such as α, β, γ.

Then

$$g_1^{2^{s_1-1}} g_2^{2^{s_2-1}} g_3^{2^{s_3-1}} \equiv \alpha\beta\gamma \equiv 1 \, [\text{mod } (1+i)^\lambda],$$

where

$$2^{s_1-1} \not\equiv 0 \pmod{2^{s_1}},$$

$$2^{s_2-1} \not\equiv 0 \pmod{2^{s_2}},$$

$$2^{s_3-1} \not\equiv 0 \pmod{2^{s_3}},$$

and therefore the three generators must not belong to three such groups.

Finally, we can see that if the three generators are taken from three different groups, excluding the seven sets of three groups, then

$$g_1^{j_1} g_2^{j_2} g_3^{j_3} \equiv 1 \, [\text{mod } (1+i)^\lambda]$$

is not possible unless

$$j_1 \equiv 0 \pmod{2^{s_1}},$$

$$j_2 \equiv 0 \pmod{2^{s_2}},$$

$$j_3 \equiv 0 \pmod{2^{s_3}}.$$

Lemma (i.) shows that $g_1^{j_1}$, $g_2^{j_2}$, $g_3^{j_3}$ belong to the same groups as do g_1, g_2, g_3. Suppose that these are α, β, and δ.

The Lemmas (iii.) and (iv.) show that the group to which $g_1^{j_1} g_2^{j_2} g_3^{j}$ belongs is one of

$$\alpha,\ \beta,\ \delta,\quad \alpha\beta,\ \alpha\delta,\ \beta\delta,\quad \text{or}\quad \alpha\beta\delta,$$

i.e.,

$$\alpha,\ \beta,\ \delta,\quad \gamma,\ \epsilon,\ \eta,\quad \text{or}\quad \theta,$$

and in no case is the product congruent to unity, save when each factor is so separately.

The result, therefore, is that for modulus $(1+i)^\lambda$ we have to take three generators with the exponents determined in the last proposition, and such that the product of the three numbers with exponent 2 that they separately produce shall not be congruent to unity.

Example.—Mod $(1+i)^8$. $\Phi(1+i)^8 = 2^7$.

The exponents of the generators are

$$2^3,\ 2^2,\ 2^2.$$

The 2^6 numbers with exp 2^3 are

$$\left.\begin{matrix} 1+2i, & 3+2i \\ 2+i, & 2+3i \end{matrix}\right\} (\text{mod } 4).$$

The $2^5 + 2^4 + 2^3$ numbers with exp 2^2 are

$$\left.\begin{matrix} i \\ 3i \end{matrix}\right\} (\text{mod } 4) \text{ and } 3,\ 5,\ 3+4i,\ 5+4i,\ 1+4i,\ 7+4i\ (\text{mod } 8).$$

The $2^2 + 2 + 1$ numbers with exp 2 are

$$15,\ 9,\ 7,\ 1+8i,\ 15+8i,\ 9+8i,\ 7+8i.$$

If of these we take

$$2+i \text{ with exp } 8,$$
$$3 \text{ with exp } 4,$$

and

$$i \text{ with exp } 4,$$

we have

$$(2+i)^4 \equiv 9+8i\ [\text{mod } (1+i)^8],$$
$$3^2 \equiv 9\ [\text{mod } (1+i)^8],$$

and

$$i^2 \equiv 15\ [\text{mod } (1+i)^8],$$

and

$$9+8i \,.\, 9 \,.\, 15 \equiv 15+8i \not\equiv 1\ [\text{mod } (1+i)^8],$$

therefore, $2+i$, 3, and i generate the 2^7 numbers.

Example.—Mod $(1+i)^9$. $\Phi(1+i)^9 = 2^8$. The three generators have exponents $2^3, 2^3, 2^2$.

The $2^7 + 2^6$ numbers with exp 2^3 are (see Proposition xv.)—

$$\equiv 7+2i,\ 5+2i,\ 6+3i,\ 6+i,\ 5,\ 3,\ 4+i,\ 3i,\ 3+2i,\ 1+2i,\ 2+3i,\ 2+i\,[\text{mod }(1+i)^5].$$

The $2^5 + 2^4 + 2^3$ numbers with exp 2^2 are

$$\equiv \pm i\,[\text{mod }(1+i)^5] \text{ and } 7,\ 9,\ 3+4i,\ 5+4i,\ 11+4i,\ 13+4i\,[\text{mod }(1+i)^7].$$

The $2^2 + 2 + 1$ numbers with exp 2, are

$$15,\ 17,\ 31,\ 7+8i,\ 23+8i,\ 25+8i,\ 9+8i.$$

If of these we take

$$2+i \text{ with exp } 8,$$
$$3 \text{ with exp } 8,$$

and

$$i \text{ with exp } 4,$$

we have

$$\left.\begin{aligned} (2+i)^4 &\equiv 9+8i \\ 3^4 &\equiv 17 \\ i^2 &\equiv 15 \end{aligned}\right\} \text{ and } 15\,.\,17\,.\,(9+8i) \equiv 7+8i \not\equiv 1.$$

Therefore $2+i$, 3, and i generate the 2^8 numbers.

(xvii.) From Propositions ix., xii., xiii., and xiv. the exponent of a number for any modulus (to which it is prime) is readily determined.

Let the modulus be expressed as a product of powers of its prime factors,

$$m = (1+i)^\kappa P_1^{\lambda_1} P_2^{\lambda_2} \ldots Q_1^{\mu_1} Q_2^{\mu_2} \ldots,$$

where $P_1, P_2, \ldots$ are pure primes, and $Q_1, Q_2, \ldots$ are mixed primes, and equal to $\alpha_1 + \beta_1 i,\ \alpha_2 + \beta_2 i \ldots$

Then, by Proposition ix., the exponent of any number a is the L.C.M. of its separate exponents for the moduli

$$(1+i)^\kappa,\ P_1^{\lambda_1},\ P_2^{\lambda_2}, \ldots Q_1^{\mu_1},\ Q_2^{\mu_2} \ldots$$

The greatest exponent possible.—The greatest exponent for mod $(1+i)^\kappa$ is

$$1 \text{ if } \kappa = 1,$$
$$2 \text{ if } \kappa = 2,$$
$$4 \text{ if } 2 < \kappa < 8,$$
$$\ldots\ldots\ldots\ldots$$
$$2^{\kappa'-1} \text{ if } 8 \leqq \kappa = 2\kappa' \text{ or } 2\kappa' + 1.$$

The greatest exponent for mod $P_1^{\lambda_1}$ is

$$P_1^2 - 1 \text{ if } \lambda_1 = 1,$$
$$P_1^{\lambda_1 - 1}(P_1^2 - 1) \text{ if } \lambda_1 > 2.$$

The greatest exponent for mod $Q_1^{\mu_1}$ is

$$\alpha_1^2 + \beta_1^2 - 1 \text{ if } \mu_1 = 1,$$
$$(\alpha_1^2 + \beta_1^2)^{\mu_1 - 1}(\alpha_1^2 + \beta_1^2 - 1) \text{ if } \mu_1 > 1,$$

and the greatest exponent for mod m is the L.C.M. of these separate greatest exponents.

Primitive roots exist when the greatest exponent is equal to $\Phi(m)$, and

$$\Phi(m) = \Phi(1+i)^{\kappa} \,.\, \Phi(P_1^{\lambda_1}) \,.\, \Phi(P_2^{\lambda_2}) \ldots \Phi(Q_1^{\mu_1})\, \Phi(Q_2^{\mu_2}) \ldots$$

and

$$\begin{aligned} \Phi(1+i)^{\kappa} &= 1 \text{ if } \kappa = 1 \\ &= 2^{\kappa - 1} \text{ if } \kappa > 1, \\ \Phi(P_1^{\lambda_1}) &= P_1^2 - 1 \text{ if } \lambda_1 = 1 \\ &= P_1^{2(\lambda_1 - 1)}(P_1^2 - 1) \text{ if } \lambda_1 > 2, \\ \Phi(Q_1^{\mu_1}) &= \alpha_1^2 + \beta_1^2 - 1 \text{ if } \mu_1 = 1 \\ &= (\alpha_1^2 + \beta_1^2)^{\mu_1 - 1}(\alpha_1^2 + \beta_1^2 - 1). \end{aligned}$$

The only cases in which the greatest exponent can be equal to $\Phi(m)$ are those in which the separate exponents are each equal to the Φ of the modulus they refer to and are also co-prime.

Hence we have the following moduli possessed of primitive roots :—

(1) The moduli $1 + i$, $(1 + i)^2$, $(1 + i)^3$;
(2) Any pure prime and $(1 + i) \times$ any pure prime ;
(3) A power of a mixed prime and $(1 + i) \times$ a power of a mixed prime.

Example.—To find the exponent of $3 + 2i$ for mod 1000.

$$1000 = 2^3 \,.\, 5^3 = -(1+i)^6\,(2+i)^3\,(1+2i)^3.$$

The exp of $3 + 2i$ for mod $(1 + i)^6$ is 4.

$$3 + 2i \equiv 1 \,(\text{mod } 2 + i),$$

and therefore has exponent 1.

$$(3 + 2i)^1 \not\equiv 1 \,[\text{mod } (2 + i)^2]$$

therefore

$$3 + 2i \text{ has exp } 5^2 \text{ for mod } (2 + i)^3.$$

$$3 + 2i \equiv 2 \pmod{1 + 2i},$$

and therefore has exp 4.

$$(3 + 2i)^4 \equiv 21 \,[\text{mod } (1 + 2i)^2]$$

$$\not\equiv 1,$$

therefore

$$3 + 2i \text{ has exp } 4 \,.\, 5^2 \text{ for mod } (1 + 2i)^3.$$

The exponent required is the L.C.M. of 4, 5^2 and $4 \,.\, 5^2 = 100$.

Therefore the exponent of $3 + 2i$ for mod 1000 is 100.

(xviii.) Proof identical with (18).

If a be not prime to m and $m = p\mathrm{P}$ where p consists of powers of those primes which occur in a, and P is prime to a, then the series of residues

$$a, a^2, a^3, \ldots a^r, \ldots a^{r+t}, \ldots \pmod{m}$$

consists of periods of t terms, the first period beginning at the r^{th} term: where t is the exponent of a for mod P, and r is the least number that makes a^r divisible by p.

Corollary.—When $a \equiv 1 \pmod{\mathrm{P}}$ $t = 1$ and the period consists of one term.

When a is divisible by p the first period starts from the first term.

When both these conditions hold good then every power of a is $\equiv a \pmod{m}$.

Example.—Residues of powers of $2 + i$ for mod 10.

$$\begin{aligned} 10 &= -(1 + i)^2 (2 + i)(1 + 2i), \\ p &= 2 + i, \\ \mathrm{P} &= (1 + i)^2 (1 + 2i), \end{aligned}$$

therefore $r = 1$, and t is the exponent of $2 + i$ for mod $(1 + i)^2 (1 + 2i)$.

Now

$$\left.\begin{aligned} &2 + i \equiv i \,[\text{mod } (1 + i)^2] \text{ and therefore has exp } 2 \\ \text{and} \quad &2 + i \equiv 4 \pmod{1 + 2i} \quad ,, \quad ,, \quad ,, \quad 2 \end{aligned}\right\}$$

therefore

$$t = 2.$$

The period consists of two terms and the first period begins at the first term

$$\begin{aligned} &2 + i, \\ (2 + i)^2 &\equiv 3 + 4i, \\ (2 + i)^3 &\equiv 2 + i, \\ &\&\text{c.} \end{aligned}$$

Example.—Residues of powers of $(1 + i)$ for mod $100 = (1 + i)^4 (2 + i)^2 (1 + 2i)^2$

$$p = (1 + i)^4,$$

and therefore

$$r = 4,$$
$$\mathrm{P} = (2 + i)^2 (1 + 2i)^2.$$

$$1 + i \text{ has exp } 4 \bmod 2 + i \text{ and } (1 + i)^4 \not\equiv 1 \; [\bmod\, (2 + 1)^2],$$

therefore

$$1 + i \text{ has exp } 20 \bmod (2 + i)^2.$$

Similarly

$$1 + i \text{ has exp } 4 \bmod 1 + 2i \text{ and } (1 + i)^4 \not\equiv 1 \; [\bmod\, (1 + 2i)^2],$$

therefore

$$1 + i \text{ has exp } 20 \bmod (1 + 2i)^2,$$

and therefore

$$t = 20.$$

The residues are

$1 + i$	$2i$	$98 + 2i$	96	$96 + 96i$	$92i$	$8 + 92i$	16	$16 + 16i$	$32i$
		$68 + 32i$	36	$36 + 36i$	$72i$	$28 + 72i$	56	$56 + 56i$	$12i$
		$88 + 12i$	76	$76 + 76i$	$52i$	$48 + 52i.$			

Example.—The residues of the powers of $688 + 784i$ for mod 1000.

$$1000 = -(1 + i)^6 (2 + i)^3 (1 + 2i)^3.$$
$$688 + 784i \equiv 0 \; [\bmod\, (1 + i)^6].$$
$$688 + 784i \equiv 688 - 57\,(784) \; [\bmod\, (2 + i)^3]. \quad \text{(See preface.)}$$
$$\equiv 0 \qquad [\bmod\, (2 + i)^3].$$

and

$$688 + 784i \equiv 688 + 57\,(784) \; [\bmod\, (1 + 2i)^3].$$
$$\equiv 1 \qquad [\bmod\, (1 + 2i)^3].$$

Hence, $r = 1$ and $t = 1$, and so all powers of the number $688 + 784i$ are congruent to itself for mod 1000.

688	688	784
688	784	784
504	752	136
04	04	72
8	6	8
344	392	656
	2	
	784	

therefore

$$(688 + 784i)^2 \equiv (344 - 656 + 784i) \pmod{1000}$$
$$\equiv 688 + 784i \pmod{1000}.$$

(xix. and xx.) The proofs and results are the same as in (19) and (20).

Example.—Mod $10 = 2.\ 5 = -(1+i)^2(2+i)(1+2i)$.

To find a so that

$$a \equiv \alpha_1 \,[\text{mod } (1+i)^2]$$
$$\equiv \alpha_2 \,[\text{mod } (2+i)]$$
$$\equiv \alpha_3 \,[\text{mod } (1+2i)].$$

We shall have

$$a \equiv \alpha_1\xi_1 + \alpha_2\xi_2 + \alpha_3\xi_3 \pmod{10},$$

where ξ_1, ξ_2, ξ_3 are found thus:—

$$\xi_1 = (2+i)(1+2i)\,x_1 \equiv 1 \,[\text{mod } (1+i)^2],$$
$$5i\,x_1 \equiv 1 \,[\text{mod } (1+i)^2],$$
$$i\,x_1 \equiv 1 \,[\text{mod } (1+i)^2],$$
$$x_1 \equiv i,$$

and therefore

$$\xi_1 \equiv 5 \pmod{10}.$$

$$\xi_2 = (1+i)^2(1+2i)\,x_2 \equiv 1 \;(\text{mod } 2+i),$$
$$(2i-4)\,x_2 \equiv 1 \;(\text{mod } 2+i),$$
$$-8x_2 \equiv 1 \;(\text{mod } 2+i),$$
$$x_2 \equiv 3 \;(\text{mod } 2+i),$$

and therefore

$$\xi_2 \equiv 8 + 6i \pmod{10}.$$

$$\xi_3 = (1+i)^2(2+i)\,x_3 \equiv 1 \;(\text{mod } 1+2i),$$
$$(4i-2)\,x_3 \equiv 1 \;(\text{mod } 1+2i),$$
$$-4x_3 \equiv 1 \;(\text{mod } 1+2i),$$
$$x_3 \equiv 1 \;(\text{mod } 1+2i),$$

and therefore

$$\xi_3 \equiv 8 + 4i \pmod{10}.$$

Hence

$$a \equiv 5\alpha_1 + (8+6i)\,\alpha_2 + (8+4i)\,\alpha_3 \pmod{10},$$

e.g., if

$$\left.\begin{array}{l} \alpha_1 \equiv 1 \,[\text{mod } (1+i)^2] \\ \alpha_2 \equiv 4 \;(\text{mod } 2+i) \\ \alpha_3 \equiv 3 \;(\text{mod } 1+2i) \end{array}\right\}$$

then

$$\begin{aligned} a &\equiv 5 + (8 + 6i)\,4 + (8 + 4i)\,.\,3\,.\,(\text{mod } 10), \\ &\equiv 5 + 2 + 4i + 4 + 2i\ (\text{mod } 10), \\ &\equiv 1 + 6i\ (\text{mod } 10). \end{aligned}$$

(xxi.) The number of numbers which belong to a given exponent when the modulus is a power of a prime.

We have three cases to consider

(1) When the modulus is a power of a pure prime.
(2) When the modulus is a power of a mixed prime.
(3) When the modulus is a power of $1 + i$.

(1.) We saw in Proposition xii*a*, that for the modulus p^λ we can generate the $\Phi(p^\lambda) = p^{2(\lambda-1)}(p^2 - 1)$ residues prime to the modulus by three generators

and
$$\left.\begin{array}{l} f \text{ and } f' \text{ each with exp } p^{\lambda-1} \\ h \text{ with exp } p^2 - 1. \end{array}\right\}$$

How many of the residues have exponent $p^s t$, where $s \not> \lambda - 1$ and t divides $p^2 - 1$?

Of the $p^2 - 1$ powers of h, $\phi(t)$ have exponent t.

Of the $p^{\lambda-1}$ powers of f, p^s have exponent a power of $p \not> p^s$.

Of the $p^{\lambda-1}$ powers of f', p^s have exponent a power of $p \not> p^s$.

Therefore f and f' generate p^{2s} numbers with exponent $\not> p^s$, and similarly p^{2s-2} numbers with exponent $\not> p^{s-1}$.

Therefore f and f' generate $p^{2s} - p^{2s-2}$ numbers with exponent p^s.

Therefore f, f', and g generate $(p^{2s} - p^{2s-2})\,\phi(t)$ numbers with exponent $p^s t$, *i.e.*, the number of numbers with exponent $p^s t$ mod p^λ is $(p^{2s} - p^{2s-2})\,\phi(t)$.

In particular the number of numbers with exponent p^s is $p^{2s} - p^{2s-2}$, and the number of numbers with exponent t is $\phi(t)$ if t is prime to p.

(2.) Any power of a mixed prime, $(\alpha + \beta i)^\lambda$, has primitive roots, and hence, as in (21), the number of numbers with exponent t [any divisor of $(\alpha^2 + \beta^2)^\lambda - (\alpha^2 + \beta^2)^{\lambda-1}$] is $\phi(t)$.

(3.) The number of numbers with exponent a given power of 2 for modulus $(1 + i)^\nu$ was found completely in Propositions xiv. and xv.

(xxi*a*.) It will be convenient for the succeeding propositions to express the number of numbers which have a given exponent for modulus $(1 + i)^\lambda$, in terms of the exponents of the generators. By so doing we shall avoid the detailed discussion of the cases arising from different values of λ, which was necessary in Part I.

Suppose 2^κ, $2^{\kappa'}$, $2^{\kappa''}$ are the exponents of the generators.

The exponent of the product of any powers of the generators is equal to the highest exponent of the three (Proposition viii.).

The generator with exponent 2^κ generates

$$2^s \text{ numbers with exp} \ngtr 2^s \text{ if } \kappa > s,$$
$$2^\kappa \text{ numbers with exp} \ngtr 2^s \text{ if } \kappa \leqq s.$$

Suppose by $(\kappa)_s$ we denote that κ is to be replaced by s if κ exceeds s. Then in either case the generator with exponent 2^κ generates

$$2^{(\kappa)_s} \text{ numbers with exp} \ngtr 2^s.$$

Similarly the two other generators generate respectively

$$2^{(\kappa')_s} \text{ numbers with exp} \ngtr 2^s,$$

and

$$2^{(\kappa'')_s} \text{ numbers with exp} \ngtr 2^s.$$

Therefore the three generators generate

$$2^{(\kappa+\kappa'+\kappa'')_s} \text{ numbers with exp} \ngtr 2^s,$$

i.e., there are, for modulus $(1+i)^\lambda$,

$$2^{(\kappa+\kappa'+\kappa'')_s} \text{ numbers with exp} \ngtr 2^s.$$

Similarly there are

$$2^{(\kappa+\kappa'+\kappa'')_{s-1}} \text{ numbers with exp} \ngtr 2^{s-1}.$$

Hence there are

$$2^{(\kappa+\kappa'+\kappa'')_s} - 2^{(\kappa+\kappa'+\kappa'')_{s-1}}$$

numbers with exponent 2^s for modulus $(1+i)^\lambda$.

This result clearly holds good when one or two of the κ's is absent, as is the case when λ is less than 5.

(xxii.) The number of numbers, for modulus m, each of which has as exponent some power of a prime p, p being a divisor of $\Phi(m)$.

Let

$$m = (1+i)^\kappa P_1^{\lambda_1} P_2^{\lambda_2} \dots Q_1^{\mu_1} Q_2^{\mu_2} \dots$$

where P_1, P_2, ... are pure primes and Q_1, Q_2, ... are mixed primes.

$$\Phi(m) = \Phi(1+i)^\kappa \,.\, \Phi(P_1^{\lambda_1}) \,.\, \Phi(P_2^{\lambda_2}) \dots \Phi(Q_1^{\mu_1}) \, \Phi(Q_2^{\mu_2}) \dots$$
$$\Phi(1+i)^\kappa = 2^{\kappa_0} 2^{\kappa_0'} 2^{\kappa_0''}$$

where 2^{κ_0}, $2^{\kappa_0'}$, $2^{\kappa_0''}$, are the exponents of the generators for mod $(1+i)^\kappa$, and suppose that

$$\Phi(P_1^{\lambda_1}) = P_1^{2(\lambda_1-1)}(P_1^2-1) = 2^{\kappa_1} p^{l_1} q^{m_1} \dots$$
$$\Phi(P_2^{\lambda_2}) = P_2^{2(\lambda_2-1)}(P_2^2-1) = 2^{\kappa_2} p^{l_2} q^{m_2} \dots$$
$$\&c. \qquad\qquad \&c.$$

With regard to these we shall follow a convention which will be useful in simplifying the next proposition.

Firstly, we write $2^{\kappa_0}2^{\kappa_0'}2^{\kappa_0'}$, and not $2^{\overline{\kappa_0 + \kappa_0' + \kappa_0''}}$. Thus the value of $(\Sigma\kappa)_s$ will be $(\kappa_0 + \kappa_0' + \kappa_0'' + \kappa_1 + \kappa_2 + \ldots)_s$, and not $(\overline{\kappa_0 + \kappa_0' + \kappa_0''} + \kappa_1 + \kappa_2 + \ldots)_s$.

Secondly, in $2^{\kappa_1}p^{l_1}q^{m_1}\ldots$ occurs the prime P_1 raised to the power $2(\lambda_1 - 1)$.

We shall suppose it written $P_1^{\lambda_1 - 1} \,.\, P_1^{\lambda_1 - 1}$, and not $P_1^{2(\lambda_1 - 1)}$.

For the rest of the principal factors no such arrangement is necessary.

Let

$$\begin{aligned} \Phi(Q_1^{\mu_1}) &= 2^{\kappa_1'}p_1^{l_1'}q_1^{m_1'}\ldots \\ \Phi(Q_2^{\mu_2}) &= 2^{\kappa_2'}p_1^{l_2'}q_1^{m_2'}\ldots \\ \&c. \qquad & \qquad \&c. \end{aligned}$$

As in (22) the number of numbers which have some power of p as exponent is the product of the number of such numbers for each separate modulus $(1 + i)^\kappa$, $P_1^{\lambda_1}$, &c.

$$\left.\begin{array}{llllll} \text{Now the number of numbers for mod} & P_1^{\lambda_1} & \text{is the power of } p \text{ in} & \Phi(P_1^{\lambda_1}) \\ \text{,,} \quad \text{,,} \quad \text{,,} & P_2^{\lambda_2} & \text{,,} \quad \text{,,} & \Phi(P_2^{\lambda_2}) \\ \text{,,} \quad \text{,,} \quad \text{,,} & Q_1^{\mu_1} & \text{,,} \quad \text{,,} & \Phi(Q_1^{\mu_1}) \end{array}\right\} \text{Prop. (xxi.).}$$

&c.

Hence the number of numbers with exponent a power of p is $p^{\Sigma(l)}$.

In particular the number of numbers with exponent a power of 2 is $2^{\Sigma(\kappa)}$.

(xxiii.) The number of numbers having a given exponent p^s for modulus m, p^s being a divisor of the greatest exponent.

Any such number has a power of p or unity for its exponent for each of the moduli $(1 + i)^\kappa$, $P_1^{\lambda_1}$, . . . &c., and the greatest power of p among these exponents must be p^s.

As in (23) the number of numbers, modulus $P_1^{\lambda_1}$, which have as exponent a power of p not greater than p^s is (if P_1 is not p) $p^{(l_1)_s}$.

In the particular case when P_1 is the prime p, if

$$\left.\begin{array}{l} \lambda_1 - 1 \text{ is } \geqq s \text{ there are } p^{2s} \text{ numbers, mod } P_1^{\lambda_1} \text{ with exp a power of } p \not> p^s \\ \text{and if} \\ \lambda_1 - 1 \text{ is} < s \text{ there are } p^{2(\lambda_1 - 1)} \quad \text{,,} \qquad \text{,,} \qquad \text{,,} \qquad \text{,,} \end{array}\right\}$$

In either case the number is $p^{(\overline{\lambda_1 - 1} + \overline{\lambda_1 - 1})_s}$.

Now we have arranged that in $\Phi(P_1^{\lambda_1})$ the power of P_1 (p in this case) shall be written $p^{l_1}p^{l_1}$, and not p^{2l_1}: thereby we easily express the number of numbers with exponent a power of $p \not> p^s$ for modulus $P_1^{\lambda_1}$, which is $p^{(l_1)_s}p^{(l_1)_s}$ or $p^{(l_1 + l_1)_s}$, but which is *not* $p^{(2l_1)_s}$.

For modulus $Q_1^{\mu_1}$ the number of numbers with exponent a power of $p \not> p^s$ is $p^{(l_1')_s}$.

Multiplying these numbers we get $p^{(\Sigma l)_s}$ as the number of numbers with exponent a power of $p \not> p^s$.

Hence the number of numbers with exponent p^s modulus m is

$$p^{(\Sigma l)_s} - p^{(\Sigma l)_{s-1}}.$$

Example.—Mod $3^3(3+2i)$. The greatest exponent is the L.C.M. of $3^2(3^2-1)$ and $12, = 72$.

We will find how many numbers have exponent 3^2, and how many numbers have exponent 3.

$$\Phi(3^3) = 2^3 \,.\, 3^2 \,.\, 3^2.$$

$$\Phi(3+2i) = 2^2 \,.\, 3.$$

The number of numbers with exponent 3^2 is

$$3^{(2+2+1)_2} - 3^{(2+2+1)_1}$$

$$= 3^5 - 3^3.$$

The number of numbers with exponent 3 is

$$3^{(2+2+1)_1} - 1$$

$$= 3^3 - 1.$$

Hence

$$\left.\begin{array}{ll} 3^5 - 3^3 & \text{numbers have exp } 3^2. \\ 3^3 - 1 & \text{numbers have exp } 3. \\ & \\ 1 & \text{number has exp } 1. \end{array}\right\}$$

and

(xxiii*a*.) By writing $\Phi(1+i)^\kappa$ in the form $2^{\kappa_0}2^{\kappa_0'}2^{\kappa_0''}$ we are enabled to apply exactly the same method to this case as we have to the case of any odd prime p. The result we obtain is that the number of numbers with exponent 2^s for mod m is

$$2^{(\Sigma\kappa)_s} - 2^{(\Sigma\kappa)_{s-1}}.$$

Example.—Mod $12 + 4i = i(1+i)^5(1+2i)$. Highest exponent $= 2^2$. $\Phi(m) = 2^6$.

$$\Phi(1+i)^5 = 2^2 \,.\, 2 \,.\, 2.$$

$$\Phi(1+2i) = 2^2.$$

The number of numbers with exponent 2^2

$$= 2^{(2+1+1+2)_2 - (2+1+1+2)_1}$$

$$= 2^6 - 2^4.$$

The number of numbers with exponent 2

$$= 2^{(2+1+1+2)_1} - 1$$
$$= 2^4 - 1.$$

Thus there are

$$\left.\begin{array}{llll} 2^6 - 2^4 & \text{numbers with exp} & & 4. \\ 2^4 - 1 & ,, & ,, & 2. \\ 1 & ,, & ,, & 1. \end{array}\right\}$$

Corollary to xxiii. and xxiii*a*.—The number of numbers that belong to any exponent is simply the product of the number of numbers that belong to each of its principal factors as exponents.

Thus, for mod m, the number of numbers with exp $t = p^s q^\sigma \ldots$ is

$$[p^{(\Sigma l)_s} - p^{(\Sigma l)_s - 1}][q^{(\Sigma m)_\sigma} - q^{(\Sigma m)_\sigma - 1}] \ldots$$

Example.—Mod $(1 + i)^6 . 3^2 (3 + 2i)(4 + i) = - i . 72 (10 + 11i)$.

$$\Phi (1 + i)^6 = 2.\ 2^2.\ 2^2.$$
$$\Phi (3^2) = 2^3.\ 3.\ 3.$$
$$\Phi (3 + 2i) = 2^2.\ 3.$$
$$\Phi (4 + i) = 2^4.$$

The highest exponent is $2^4. 3^3$.

$$\Phi (m) = 2^{14}.\ 3^3.$$

The numbers κ are 1. 2. 2. 3. 2. 4.

$$(\Sigma\kappa)_4 = 14,$$
$$(\Sigma\kappa)_3 = 13,$$
$$(\Sigma\kappa)_2 = 11,$$
$$(\Sigma\kappa)_1 = 6,$$
$$(\Sigma\kappa)_0 = 0.$$

Therefore

$$\begin{array}{lllll} 2^{14} - 2^{13} & \text{numbers} & \text{have} & \text{exp} & 2^4, \\ 2^{13} - 2^{11} & ,, & ,, & ,, & 2^3, \\ 2^{11} - 2^6 & ,, & ,, & ,, & 2^2, \\ 2^6 - 1 & ,, & ,, & ,, & 2. \end{array}$$

The numbers l for the prime 3 are 1. 1. 1.

$$(\Sigma l)_1 = 3,$$
$$(\Sigma l)_0 = 0,$$

therefore $3^3 - 1$ numbers have exp 3.

From these we deduce that

$$\begin{array}{llll}(3^3-1)(2^{14}-2^{13}) & \text{numbers have exp} & 3.\ 2^4, \\ (3^3-1)(2^{13}-2^{11}) & \quad ,, \quad ,, \quad ,, & 3.\ 2^3, \\ (3^3-1)(2^{11}-2^{6}) & \quad ,, \quad ,, \quad ,, & 3.\ 2^2, \\ (3^3-1)(2^{6}-1) & \quad ,, \quad ,, \quad ,, & 3.\ 2. \end{array}$$

Including 1 which has exponent 1, this makes the complete set of $2^{14}.\ 3^3$ numbers.

(xxiv.) A special set of generators which generate the $\Phi(m)$ numbers, modulus m.

$$m = (1+i)^\kappa \mathrm{P}_1^{\lambda_1} \ldots \mathrm{Q}_1^{\mu_1} \ldots$$

Three numbers ϕ, ϕ', ϕ'', generate the residues for modulus $(1+i)^\kappa$. (Propositions xiii. and xvi.) Two numbers g_1, f_1, generate the residues for modulus $\mathrm{P}_1^{\lambda_1}$. (Proposition xii*a*.), &c. One number g'_1 generates the residues for modulus $\mathrm{Q}_1^{\mu_1}$. (Proposition xii.), &c.

Suppose any number a modulus m is

$$\equiv \alpha_0 \,[\mathrm{mod}\,(1+i^\kappa)]$$
$$\equiv \alpha_1 \,(\mathrm{mod}\ \mathrm{P}_1^{\lambda_1}),$$
&c.
$$\equiv \alpha'_1 \,(\mathrm{mod}\ \mathrm{Q}_1^{\mu_1}),$$
&c.

Then

$$a \equiv \alpha_0\xi_0 + \alpha_1\xi_1 + \ldots + \alpha'_1\xi'_1 + \ldots\ (\mathrm{mod}\ m). \quad \text{(Proposition xix.)}$$

If now

$$\alpha_0 \equiv \phi^{i_0}\phi'^{i'_0}\phi''^{i''_0}\,[\mathrm{mod}\,(1+i)^\kappa]$$
$$\alpha_1 \equiv g_1^{i_1} f_1^{j_1}\,(\mathrm{mod}\ \mathrm{P}_1^{\lambda_1}),$$
&c.
$$\alpha'_1 \equiv g'^{i'_1}_1\,(\mathrm{mod}\ \mathrm{Q}_1^{\mu_1}),$$
&c.

Thus

$$\begin{aligned} a &\equiv \phi^{i_0}\phi'^{i'_0}\phi''^{i''_0}\xi_0 + g_1^{i_1}f_1^{j_1}\xi_1 + \ldots + g'^{i'_1}_1\xi'_1 + \ldots\ (\mathrm{mod}\ m) \\ &\equiv [\phi\xi_0 + \xi_1 + \ldots + \xi'_1 + \ldots]^{i_0}[\phi'\xi_0 + \xi_1 + \ldots + \xi'_1 + \ldots]^{i'_0} \\ &\qquad [\phi''\xi_0 + \xi_1 + \ldots + \xi'_1 + \ldots]^{i''_0}[\xi_0 + g_1\xi_1 + \ldots + \xi'_1 + \ldots]^{i_1} \\ &\qquad\quad [\xi_0 + f_1\xi_1 + \ldots]^{j_1} \ldots [\xi_0 + \xi_1 + \ldots + g'_1\xi'_1 + \ldots]^{i'_1} \ldots\ (\mathrm{mod}\ m) \\ &\equiv [(\phi-1)\,\xi_0 + 1]^{i_0}[(\phi'-1)\,\xi_0 + 1]^{i'_0}[(\phi''-1)\,\xi_0 + 1]^{i''_0}[(g_1-1)\,\xi_1 + 1]^{i_1} \\ &\qquad\qquad [(f_1-1) + 1]^{j_1} \ldots [(g'_1-1) + 1]^{i'_1} \ldots\ (\mathrm{mod}\ m), \end{aligned}$$

where the numbers in the square brackets are a set of generators whose exponents are, in order, κ_0, κ'_0, κ''_0, $P_1^{\lambda_1-1}(P_1^2-1)$, $P_1^{\lambda_1-1}, \ldots \Phi(Q_1^{\mu_1}) \ldots$ whose product is equal to $\Phi(m)$.

Example.—Mod $10 = -(1+i)^2(2+i)(1+2i)$

i with exp 2 generates the 2 numbers mod $(1+i)^2$
2 ,, 4 ,, 4 ,, $2+i$
2 ,, 4 ,, 4 ,, $1+2i$.

Hence the following will generate the $\Phi(10) = 32$ numbers, mod 10, viz.,

$$\left.\begin{array}{r} i\xi_1 + \xi_2 + \xi_3 \\ \xi_1 + 2\xi_2 + \xi_3 \\ \xi_1 + \xi_2 + 2\xi_3 \end{array}\right\} \text{mod } 10,$$

where

$\xi_1 = 5 \quad \xi_2 = 8 + 6i \quad \xi_3 = 8 + 4i$. (See Example, Proposition xix.)

$$\left.\begin{array}{l} 5i + 8 + 6i + 8 + 4i \equiv 6 + 5i \\ 5 + 2(8 + 6i) + 8 + 4i \equiv 9 + 6i \\ 5 + 8 + 6i + 2(8 + 4i) \equiv 9 + 4i \end{array}\right\} (\text{mod } 10).$$

Hence

$$\left.\begin{array}{lcc} 9 + 4i & \text{with exp} & 4 \\ 9 + 6i & ,, & 4 \\ 6 + 5i & ,, & 2 \end{array}\right\} \text{generate the 32 residues.}$$

The indices corresponding to each of the 32 numbers are given in the following table.

Numbers.	Indices of			Numbers.	Indices of		
	$6 + 5i$.	$9 + 6i$.	$9 + 4i$.		$6 + 5i$.	$9 + 6i$.	$9 + 4i$.
1	0	0	0	$6 + 5i$	1	0	0
$9 + 4i$	0	0	1	$4 + 9i$	1	0	1
$5 + 2i$	0	0	2	$7i$	1	0	2
$7 + 8i$	0	0	3	$2 + 3i$	1	0	3
$9 + 6i$	0	1	0	$4 + i$	1	1	0
7	0	1	1	$2 + 5i$	1	1	1
$3 + 8i$	0	1	2	$8 + 3i$	1	1	2
$5 + 4i$	0	1	3	$9i$	1	1	3
$5 + 8i$	0	2	0	$3i$	1	2	0
$3 + 2i$	0	2	1	$8 + 7i$	1	2	1
9	0	2	2	$4 + 5i$	1	2	2
$1 + 6i$	0	2	3	$6 + i$	1	2	3
$7 + 2i$	0	3	0	$2 + 7i$	1	3	0
$5 + 6i$	0	3	1	i	1	3	1
$1 + 4i$	0	3	2	$6 + 9i$	1	3	2
3	0	3	3	$8 + 5i$	1	3	3

E.g., $6 + i \equiv (6 + 5i)(9 + 6i)^2(9 + 4i)^3$ (mod 10).

(xxv.) Proposition (25) is completely applicable to the case of complex numbers and moduli. The result arrived at we may re-state as follows:—The most general set of numbers which generate the $\Phi(m)$ residues for modulus m must always be constructed in this manner, viz., we must form

$$\left.\begin{array}{l}\text{a set of } p\text{-power-exponent generators}\\ \text{a set of } q\text{-power-exponent generators}\\ \qquad\&\text{c.} \qquad\qquad \&\text{c.}\end{array}\right\} p,\ q,\ \ldots \text{ being the prime factors of } \Phi(m),$$

each generator must then be formed by taking numbers from these sets, not more than one from each, and forming their product. Each number, moreover, in these subsidiary sets is to appear once and once only as a factor of one of the generators that are thus formed.

It remains to investigate the most general mode of formation of a set of p-power-exponent generators.

(xxvi.) The proof of Proposition (26) holds good for complex numbers and moduli. It shows that the exponents of any set of p-power-exponent generators must be the same set of powers of p as those which occur in the Φ's of the principal factors of m; *i.e.*, they are what have been denoted by $p^{l_1}, p^{l_2}, \ldots p^{l'_1}, p^{l'_2}; \ldots$ (see Proposition xxii., in which the convention stated must be strictly attended to). The convention of Proposition xxii. makes the treatment of the 2-power-exponent numbers uniform with that of the p-power-exponent numbers; hence the same result is true for the 2-power-exponent numbers, viz., that the exponents of any set of 2-power-exponent generators must be $2^{\kappa_0}, 2^{\kappa'_0}, 2^{\kappa''_0}, 2^{\kappa_1}, \ldots 2^{\kappa'_1} \ldots$

The least number of generators for a given modulus m.

As in (26) we see that the least number of generators is equal to the number of terms of that row which contains most among the following:—

$$\begin{array}{rrrrrrr}\kappa_0 \ \kappa'_0 \ \kappa''_0 & \kappa_1 & \kappa_2 \ldots & \kappa'_1 & \kappa'_2 \ldots\\ & l_1 & l_2 \ldots & l'_1 & l'_2 \ldots\\ & m_1 & m_2 \ldots & m'_1 & m'_2 \ldots\end{array}$$

Consider first the set of numbers, $\kappa_0 \ \kappa'_0 \ \kappa''_0 \ \kappa_1 \ldots \kappa_1 \ldots$

Since P_1 is an odd prime, therefore

$$\Phi(P_1^{\lambda_1}) = P_1^{2(\lambda_1-1)}(P_1^2 - 1)$$

is even, and therefore κ_1 always occurs.

Similarly in

$$\Phi(Q_1^{\mu_1}) = (\alpha_1^2 + \beta_1^2)^{\mu_1-1}(\alpha_1^2 + \beta_1^2 - 1)$$

$\alpha_1^2 + \beta_1^2$ is a real odd prime number, and therefore

$$\Phi\,(Q_1^{\mu_1})$$

is even, and therefore κ'_1 always occurs.

For the numbers, $\kappa_0\ \kappa'_0\ \kappa''_0$, all three occur if

$$\kappa > 4 \qquad [m = (1+i)^{\kappa} P_1^{\lambda_1} \ldots Q_1^{\mu_1} \ldots],$$

two occur if

$$\kappa = 4,$$

one occurs if

$$\kappa = 3,\ 2,\ 1,$$

none occur if

$$\kappa = 0.$$

Hence, if we denote by n the number of different prime factors, $P_1\,P_2 \ldots Q_1\,Q_2 \ldots$ of m (excluding $1 + i$) then the number of terms in the set of numbers $\kappa_0\ \kappa'_0\ \kappa''_0\ \kappa_1 \ldots \kappa'_1 \ldots$ is

$$\begin{array}{lll} n+3 & \text{if} & \kappa > 4, \\ n+2 & \text{if} & \kappa = 4, \\ n+1 & \text{if} & \kappa = 3,\ 2,\ 1, \\ n & \text{if} & \kappa = 0. \end{array}$$

These numbers give an inferior limit to the least number of generators. In all but one exceptional case the least number of generators coincides with these.

Consider next the set of numbers, $l_1\ l_2 \ldots l_1'\ l_2' \ldots$

l_1' occurs if p divides

$$\Phi\,(P_1^{\lambda_1}) = P_1^{2(\lambda_1-1)}(P_1^2 - 1).$$

If it divides

$$P_1^2 - 1$$

it occurs once. If it is identical with P_1 then it occurs twice ($l_1 = \lambda_1 - 1$), and the set of numbers would be written $l_1\ l_1\ l_2 \ldots l_1'\ l_2' \ldots$

l_2 occurs if p divides

$$\Phi\,(Q_1^{\mu_1}).$$

Therefore the number of terms in the set exceeds n (and is equal to $n + 1$) only when m is such that

$$\Phi\,(Q_1^{\mu_1}),\ \Phi\,(Q_2^{\mu_2}), \ldots\ \Phi\,(P_1^{\lambda_1}),\ \Phi\,(P_2^{\lambda_2}) \ldots$$

are all divisible by p and also one of the primes, $P_1, P_2, \ldots$ is equal to p.

If this be the case when $\kappa = 0$ the least number of generators is $n + 1$.

The result may be stated thus :—

If n be the number of different prime factors of $m = (1 + i)^{\kappa} \mathrm{P}_1^{\lambda_1} \ldots \mathrm{Q}_1^{\mu_1}, \ldots$ excluding $(1 + i)$, then the least number of generators is

$$\begin{array}{ll} n + 3 & \text{if } \kappa > 4, \\ n + 2 & \text{if } \kappa = 4, \\ n + 1 & \text{if } \kappa = 3, 2, 1, \\ n & \text{if } \kappa = 0, \end{array}$$

unless one of the primes P_1 divides $\mathrm{P}_2^2 - 1$, $\mathrm{P}_3^2 - 1, \ldots$ and $\Phi(\mathrm{Q}_1^{\mu_1})$, $\Phi(\mathrm{Q}_2^{\mu_2}), \ldots$ in which case it is $n + 1$.

(xxvii.) The formation of a set of *unitary* p-power-exponent generators for mod m.

Let a be any p-power-exponent number, and

$$a \equiv \alpha_0 \xi_0 + \alpha_1 \xi_1 + \alpha_2 \xi_2 + \ldots + \alpha'_1 \xi'_1 + \alpha'_2 \xi'_2 + \ldots \pmod{m}.$$

Then α_0, α_1, $\alpha_2, \ldots \alpha'_1, \ldots$ must each have as exponent, for its own modulus, either unity or a power of p.

Suppose first that p is not $= 2$, but an odd (real) prime.

Take

$$\begin{array}{lll} \gamma_1 & \text{with exp } p^{l_1} & (\text{mod } \mathrm{P}_1^{\lambda_1}), \\ \gamma_2 & \quad ,, \quad ,, \quad p^{l_2} & (\text{mod } \mathrm{P}_2^{\lambda_2}), \\ \text{\&c.,} & & \text{\&c.,} \end{array}$$

if in any case p is not a factor of $\Phi(\mathrm{P}^{\lambda})$ γ is $\equiv 1$.

If for one of these, say P_1, $p = \mathrm{P}_1$, then take also β_1 with exponent p^{l_1}, modulus $\mathrm{P}_1^{\lambda_1}$, as in Proposition xii., so that β_1 and γ_1, each with exponent $l_1 = \lambda_1 - 1$, generate all the p-power-exponent numbers, modulus $\mathrm{P}_1^{\lambda_1}$.

Take also

$$\begin{array}{lll} \gamma'_1 & \text{with exp } p^{l'_1}, & \text{mod } \mathrm{Q}_1^{\mu_1}, \\ \gamma'_2 & \quad ,, \quad ,, \quad p^{l'_2}, & \quad ,, \quad \mathrm{Q}_2^{\mu_2}, \\ \text{\&c.,} & & \text{\&c.} \end{array}$$

Then we have

$$\alpha_0 \equiv 1 \; [\text{mod } (1 + i)^{\kappa}],$$

and can put

$$\begin{array}{ll} \alpha_1 \equiv \gamma_1^{i_1} \beta_1^{j_1} & (\text{mod } \mathrm{P}_1^{\lambda_1}), \\ \alpha_2 \equiv \gamma_2^{i_2} & (\text{mod } \mathrm{P}_2^{\lambda_2}), \\ \quad \text{\&c.,} & \quad \text{\&c.,} \\ \alpha'_1 \equiv \gamma'^{\,l'_1}_1 & (\text{mod } \mathrm{Q}_1^{\mu_1}), \\ \alpha'_2 \equiv \gamma'^{\,i'_2}_2 & (\text{mod } \mathrm{Q}_2^{\mu_2}), \\ \text{\&c.,} & \end{array}$$

and so

$$a \equiv [(\gamma_1 - 1)\xi_1 + 1]^{i_1} [(\beta_1 - 1)\xi_1 + 1]^{j_1} [(\gamma_2 - 1)\xi_2 + 1]^{i_2} \ldots$$
$$[(\gamma'_1 - 1)\xi'_1 + 1]^{i'_1} [(\gamma'_2 - 1)\xi'_2 + 1]^{i'_2} \ldots \pmod{m}.$$

The quantities in the brackets we shall denote by $g_1 g_2 \ldots g_\mu$. Each is congruent to unity for all but one of the principal factors of m as moduli. Their exponents are the exponents of any set of p-power-exponent generators (Proposition xxvi.), viz., $p^{l_1}, p^{l_2}, \ldots$

Next let $p = 2$.

Then take ϕ, ϕ', ϕ'', generators for mod $(1 + i)^\kappa$

γ_1 a number with exp 2^{κ_1} (mod $\mathrm{P}_1^{\lambda_1}$),

&c. &c.

γ'_1 a number with exp $2^{\kappa'_1}$ (mod $\mathrm{Q}_1^{\mu_1}$),

&c. &c.

Then

$$\alpha_0 \equiv \phi^j \phi'^{j'} \phi''^{j''} \;[\mathrm{mod}\ (1 + i)^\kappa]$$
$$\alpha_1 \equiv \gamma_1^{i_1} \pmod{\mathrm{P}_1^{\lambda_1}},$$

&c.,

$$\alpha'_1 \equiv \gamma'^{\,i'_1}_1 \pmod{\mathrm{Q}_1^{\mu_1}},$$

&c.

and, therefore,

$$a \equiv [(\phi - 1)\,\xi_0 + 1]^j\, [(\phi' - 1)\,\xi_0 + 1]^{j'}\, [(\phi'' - 1)\,\xi_0 + 1]^{j''}\, [(\gamma_1 - 1)\,\xi_1 + 1]^{i_1} \ldots$$
$$[(\gamma'_1 - 1)\,\xi'_1 + 1]^{i'_1} \ldots \pmod{m},$$

and the numbers in brackets are unitary generators of the numbers, modulus m, with exponent powers of 2.

Each is congruent to unity for all but one of the principal factors of m, and their exponents are $2^{\kappa_0}\, 2^{\kappa'_0}\, 2^{\kappa''_0}\, 2^{\kappa_1}\, 2^{\kappa_2} \ldots 2^{\kappa'_1}\, 2^{\kappa_2'} \ldots$

Thus, in either case, whether p is an odd prime or equal to 2, we can form a set of p-power-exponent generators (having the exponents found to be necessary in Proposition xxvi.), such that each is congruent to unity for all but one of the principal factors of m $[(1 + i), \mathrm{P}_1^{\lambda_1}, \ldots \mathrm{Q}_1^{\mu_1} \ldots]$ as moduli.

(xxviii–xxxi.) Propositions 28–30 are concerned with a discussion of the most general mode of formation of a set of p-power-exponent generators. They are throughout completely applicable to the case of complex numbers and moduli. The result we may state as follows. Let $g_1, g_2, \ldots g_\mu$ be a set of unitary p-power-exponent generators.

Then $\Gamma_1\, \Gamma_2 \ldots \Gamma_\mu$ (with the same set of powers of p as exponents) as given by

$$\left.\begin{array}{l} \Gamma_1 \equiv g_1^{i_{11}} g_2^{i_{21}} g_3^{i_{31}} \ldots g_\mu^{i_{\mu 1}} \\ \Gamma_2 \equiv g_1^{i_{12}} g_2^{i_{22}} g_3^{i_{32}} \ldots g_\mu^{i_{\mu 2}} \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ \Gamma_\mu \equiv g_1^{i_{1\mu}} g_2^{i_{2\mu}} g_3^{i_{3\mu}} \ldots g_\mu^{i_{\mu\mu}} \end{array}\right\} \pmod{m}$$

will be independent generators provided that the determinants formed by the indices i,

$$\left.\begin{array}{l} (i_{11}\, i_{22} \ldots i_{aa}) \\ (i_{a+1\ a+1} \ldots i_{bb}) \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ (\ldots\ldots\ldots i_{\mu\mu}) \end{array}\right\} \text{ are all prime to } p.$$

The indices i which occur in any one of these determinants, are those which occur as indices of generators g all with the same exponent; the generators Γ, in which they occur, having also this same exponent.

The summary of Proposition (31) is also true of generators for complex moduli.

(xxxii. and xxxiii.) With one modification, Propositions (22) and (23) hold good for complex numbers and primes.

If in

$$ax^n \equiv b \pmod{m}$$

a and m have G.C.M κ, then

$$\frac{a}{\kappa} x^n \equiv \frac{b}{\kappa} \left(\text{mod } \frac{m}{\kappa}\right).$$

Each solution, x, of the second congruence gives N (κ) solutions of the first, viz., all the numbers $x + s\frac{m}{\kappa}$, where s is any one of the N (κ) incongruent residues for modulus κ.

The solutions of the congruences which follow are intended as examples of these propositions and also as illustrations of the Tables placed in the Appendix.

Example 1.

$$7x^3 \equiv 3 \pmod{4 + 2i}.$$

From the tables

$$\begin{array}{l} \qquad\ \ {\scriptstyle (4)\ \ (2)} \\ 3 \equiv (3.\ 0) \\ 7 \equiv (1.\ 0), \end{array}$$

therefore

$$x^3 \equiv (2.\ 0),$$

therefore

$$x \equiv (2.\ 0)$$

$$x \equiv 9 \pmod{4 + 2i}.$$

Example 2.

$$(2+i)\,x^3 \equiv 3 + 2i \pmod{9}.$$

From the tables

$$3 + 2i \equiv (\overset{(24)}{22}.\ \overset{(3)}{0})$$

$$2 + i \equiv (\ 1.\ 0),$$

therefore

$$x^3 \equiv (21.\ 0),$$

therefore, if

$$x \equiv (a.\ b),$$

$$3a \equiv 21 \pmod{24},$$

therefore

$$a \equiv 7,\ 15,\ 23 \pmod{24}$$

$$3b \equiv 0 \pmod{3},$$

therefore

$$b \equiv 0,\ 1,\ 2 \pmod{3}.$$

There are thus nine solutions, viz. :

$$\begin{array}{lll}
(7.\ 0) \equiv 1 + 7i & (15.\ 0) \equiv 7 + 7i & (23.\ 0) \equiv 4 + 7i \\
(7.\ 1) \equiv 1 + 4i & (15.\ 1) \equiv 7 + 4i & (23.\ 1) \equiv 4 + 4i \\
(7.\ 2) \equiv 1 + i & (15.\ 2) \equiv 7 + i & (23.\ 2) \equiv 4 + i
\end{array}$$

Example 3.

$$3x^3 \equiv 3 + 2i \pmod{10}.$$

From the tables

$$3 + 2i \equiv (\overset{(4)}{1}.\ \overset{(4)}{2}.\ \overset{(2)}{0})$$

$$3 \equiv (3.\ 3.\ 0),$$

therefore

$$x^3 \equiv (2.\ 3.\ 0),$$

and therefore

$$x \equiv (2.\ 1.\ 0)$$

$$x \equiv 3 + 8i.$$

Example 4.

$$3x^3 \equiv 3 + 2i \pmod{30 + 20i},$$

and so

$$3\,\frac{x^3}{3+2i} \equiv 1 \pmod{10}.$$

Let

$$x = (3 + 2i)\,\xi.$$

Then

$$3\,(3 + 2i)^2\,\xi^3 \equiv 1 \pmod{10}$$

Now

$$3 + 2i \equiv (\overset{(4)}{1}.\ \overset{(4)}{2}.\ \overset{(2)}{0}),$$

therefore

$$(3 + 2i)^2 \equiv (2.\ 0.\ 0);$$

also

$$3 \equiv (3.\ 3.\ 0),$$

therefore

$$3\,(3 + 2i)^2 \equiv (1.\ 3.\ 0),$$

therefore

$$\xi^3 \equiv (3.\ 1.\ 0),$$

therefore, if

$$\xi \equiv (a.\ b.\ c)$$

$$\left.\begin{aligned} 3a &\equiv 3 \pmod{4} \\ 3b &\equiv 1 \pmod{4} \\ 3c &\equiv 0 \pmod{2} \end{aligned}\right\} \begin{aligned} a &= 1 \\ b &= 3 \\ c &= 0 \end{aligned}$$

$$\begin{aligned} \xi &\equiv (1.\ 3.\ 0) \\ &\equiv 5 + 6i \pmod{10}, \end{aligned}$$

and therefore

$$\begin{aligned} x &\equiv (3 + 2i)(5 + 6i) \pmod{10\ \overline{3 + 2i}} \\ &\equiv 3 + 28i \\ &\equiv 103 + 8i \pmod{10 \,.\, \overline{3 + 2i}}. \end{aligned}$$

Example 5.

$$4x^5 \equiv 14 + 7i \pmod{15 + 10i}.$$

This is

$$4x^5 \equiv 7\,(2 + i) \pmod{\overline{2 + i}.\ \overline{1 + 2i}.\ \overline{3 + 2i}},$$

therefore

$$4\,\frac{x^5}{2 + i} \equiv 7 \pmod{8 + 1}.$$

Let

$$x = (2 + i)\,\xi.$$

Then

$$4\,(2 + i)^4 \xi^5 \equiv 7 \pmod{8 + i}.$$

From the tables

$$\begin{aligned} 7 &\equiv (\overset{(12)}{11}.\ \overset{(4)}{2}), \\ (2 + i) &\equiv 59 \pmod{8 + i}, \\ &\equiv (11.\ 3), \end{aligned}$$

therefore

$$\begin{aligned} (2 + i)^4 &\equiv (8.\ 0), \\ 4 &\equiv (2.\ 0), \end{aligned}$$

therefore

$$(2 + i)^4 . 4 \equiv (10.\ 0),$$

therefore

$$\xi^5 \equiv (1.\ 2),$$

therefore, if

$$\xi \equiv (a.\ b),$$

$$5a \equiv 1 \pmod{12}, \quad a \equiv 5,$$

$$5b \equiv 2 \pmod{4}, \quad b \equiv 2,$$

$$\xi \equiv (5.\ 2),$$

$$\equiv 58 \pmod{8 + i}.$$

So

$$x \equiv 58\,(2 + i) \pmod{15 + 10i}$$

$$\equiv 1 + 3i.$$

Example 6.

$$2x^2 \equiv 26 + 32i \pmod{40},$$

and therefore

$$x^2 \equiv 13 + 16i \pmod{20}.$$

Each solution of the latter gives four of the former, viz.,

$$x, \quad x + 20, \quad x + 20i, \quad x + 20 + 20i \pmod{40}.$$

The congruence is

$$x^2 \equiv -i\,(1 + 2i)^2\,(4 + i)\,[\text{mod}\ (1 + i)^4 .\ (2 + i).\ (1 + 2i)],$$

therefore

$$\frac{x^2}{1 + 2i} \equiv -i\,(1 + 2i)\,(4 + i)\,[\text{mod}\ (1 + i)^4 .\ (2 + i)].$$

Let

$$x \equiv (1 + 2i)\,\xi \pmod{20}.$$

Then

$$(1 + 2i)\,\xi^2 \equiv -i\,(1 + 2i)\,(4 + i)\,[\text{mod}\ (1 + i)^4 .\ (2 + i)],$$

and therefore

$$\xi^2 \equiv -i\,.\,(4 + i) \pmod{8 + 4i},$$

$$\equiv 1 - 4i \pmod{8 + 4i},$$

$$\xi^2 \equiv 9 \pmod{8 + 4i}.$$

From the tables

$$9 \equiv (\overset{(4)}{2}.\ \overset{(4)}{0}.\ \overset{(2)}{0}),$$

and therefore

$$\xi^2 \equiv (2.\ 0.\ 0).$$

This gives eight solutions

$$\begin{aligned} \xi &\equiv (1.\ 0.\ 0) \equiv 17, \\ &\equiv (3.\ 0.\ 0) \equiv 13, \\ &\equiv (1.\ 2.\ 0) \equiv 7, \\ &\equiv (3.\ 2.\ 0) \equiv 3, \\ &\equiv (1.\ 0.\ 1) \equiv 1 + 2i, \\ &\equiv (3.\ 0.\ 1) \equiv 17 + 2i, \\ &\equiv (1.\ 2.\ 1) \equiv 11 + 2i, \\ &\equiv (3.\ 2.\ 1) \equiv 7 + 2i. \end{aligned}$$

Hence there are eight solutions of the congruence

$$x^2 \equiv 13 + 16i \pmod{20},$$

viz.,

$$\begin{array}{cccc} 7 + 4i & 17 + 4i & 7 + 14i & 17 + 14i \\ 3 + 6i & 13 + 6i & 3 + 16i & 13 + 16i \end{array}$$

and hence there are 32 solutions of the congruence

$$2x^2 \equiv 26 + 32i \pmod{40},$$

viz.,

$$\begin{array}{rrrr} 7 + 4i & 17 + 4i & 7 + 14i & 17 + 14i \\ 27 + 4i & 37 + 4i & 27 + 14i & 37 + 14i \\ 7 + 24i & 17 + 24i & 7 + 34i & 17 + 34i \\ 27 + 24i & 37 + 24i & 27 + 34i & 37 + 34i \\ 3 + 6i & 13 + 6i & 3 + 16i & 13 + 16i \\ 23 + 6i & 33 + 6i & 23 + 16i & 33 + 16i \\ 3 + 26i & 13 + 26i & 3 + 36i & 13 + 36i \\ 23 + 26i & 33 + 26i & 23 + 36i & 33 + 36i \end{array}$$

APPENDIX.

Tables of Indices for all Moduli whose Norms do not exceed 100.

Description of Tables.

The following Appendix contains Tables of Indices for all the moduli whose norms do not exceed 100. For each modulus two tables are given: the first arranged so as to show readily the number that corresponds to given indices, the second to show what indices correspond to a given number. At the foot of any column, or the end of any row in which indices are tabulated, is placed in a bracket the exponent of the generator to which those indices refer. With each table are noted the formulæ necessary for finding to which of the numbers in the table any given number is congruent. There are also given for convenience the prime factors of the modulus, the norm, the highest exponent, the value of Φ expressed in factors which show the exponents of the generators, and the generators used in the table. All these will be found collected in the reference table next following. In this are also noted, for each modulus, the least possible number of generators and the values of the numbers ξ of Proposition xix. *E.g.*, for the modulus $5 + 5i$ we read thus :—

$$5 + 5i = -i(1 + i)(2 + i)(1 + 2i), \quad \mathrm{N}(5 + 5i) = 50, \quad \Phi(5 + 5i) = 16 = 2^2 . 2^2.$$

Highest exponent = 4. Least number of generators = 2, those used in the table being $4 + i$ and $9 + 4i$.

Also if

$$\left.\begin{aligned} a &\equiv \alpha_0 (\mathrm{mod}\ 1 + i) \\ &\equiv \alpha_1 (\mathrm{mod}\ 2 + i) \\ &\equiv \alpha_2 (\mathrm{mod}\ 1 + 2i) \end{aligned}\right\}$$

then

$$a \equiv 5\alpha_0 + (3 + i)\alpha_1 + (8 + 4i)\alpha_2 (\mathrm{mod}\ 5 + 5i).$$

The reducing formulæ (see preface, Part II.) are

$$\begin{aligned} y &\equiv \mathrm{Y} (\mathrm{mod}\ 5), \\ x &\equiv \mathrm{X} + \mathrm{Y} - y (\mathrm{mod}\ 10). \end{aligned}$$

The tables of indices for powers of $1 + i$ as moduli, up to $(1 + i)^8$, are placed at the end.

[The tables have been calculated with some care, but they have not been revised.]

m.	N (m).	Φ (m).	H.E.	No. of gens.	Gens. used.	The numbers ξ.	$d\,(\alpha^2+\beta^2)$.	d.	$-(\alpha\alpha'+\beta\beta')$.
$1+i$	2	1	1	1	1	..	2	..	1
$2 \quad =-i\,(1+i)^2$	4	2	2	1	i	..	2	2	
$2+i$ $1+2i$	5	$4=2^2$	4	1	2	..	5	..	3 2
$2+2i=-i\,(1+i)^3$	8	$4=2^2$	4	1	i	..	4	2	1
3.	9	$8=2^3$	8	1	$1+i$	..	3	3	
$3+i=-i\,(1+i)\,(1+2i)$ $1+3i=\quad(1+i)\,(2+i)$	10	$4=2^2$	4	1	3	5, 6	10	..	7 3
$3+2i$ $2+3i$	13	$12=2^2.\,3$	12	1	2	..	13	..	5 8
$4 \quad =-\,(1+i)^4$	16	$8=2.\,2^2$	4	2	i $1+2i$	..	4	4	
$4+i$ $1+4i$	17	$16=2^4$	16	1	3	..	17	..	13 6
$3+3i=\quad(1+i).\,3$	18	$8=2^3$	8	1	$1+2i$	3, 4	6	3	1
$4+2i=-i\,(1+i)^2\,(2+i)$ $2+4i=-i\,(1+i)^2\,(1+2i)$	20	$8=2.\,2^2$	4	2	$7,\ 8+i$ $7,\ 4+i$	5,.6	10	2	3 7
$5 \quad =-i\,(2+i)\,(1+2i)$	25	$16=2^2.\,2^2$	4	2	$4+i,\ 4+4i$	$3+i,\ 3+4i$	5	5	
$4+3i=-i\,(1+2i)^2$ $3+4i=\quad(2+i)^2$	25	$20=2^2.\,5$	20	1	2	..	25	..	7 18
$5+i=-i\,(1+i)\,(2+3i)$ $1+5i=\quad(1+i)\,(3+2i)$	26	$12=2^2.\,3$	12	1	7	13, 14	26	..	21 5
$5+2i$ $2+5i$	29	$28=2^2.\,7$	28	1	2	..	29	..	12 17
$4+4i=-\,(1+i)^5$	32	$16=2.\,2.\,2^2$	4	3	i $1+2i$ 3	..	8	4	1
$5+3i=-i\,(1+i)\,(1+4i)$ $3+5i=\quad(1+i)\,(4+i)$	34	$16=2^4$	16	1	3	17, 18	34	..	21 13
$6 \quad =-i\,(1+i)^2.\,3$	36	$16=2.\,2^3$	8	2	$1+4i,\ 4+3i$	3, 4	6	6	
$6+i.$ $1+6i$	37	$36=2^2.\,3^2$	36	1	2	..	37	..	31 6
$6+2i=-\,(1+i)^3\,(1+2i)$ $2+6i=-i\,(1+i)^3\,(2+i)$	40	$16=2^2.\,2^2$	4	2	$3,\ i$ $3,\ 14+i$	5, 16	20	2	7 13
$5+4i$ $4+5i$	41	$40=2^3.\,5$	40	1	6	..	41	..	9 32
$6+3i=\quad(2+i).\,3$ $3+6i=\quad(1+2i).\,3$	45	$32=2^2.\,2^3$	8	2	$1+i,\ i$ $10+2i,\ 9+2i$	6, 10	15	3	3 12
7.	49	$48=2^4.\,3$	48	1	$2+i$	..	7	7	
$7+i=-i\,(1+i)\,(2+i)^2$ $1+7i=-i\,(1+i)\,(1+2i)^2$	50	$20=2^2.\,5$	20	1	3	25, 26	50	..	43 7
$5+5i=-i\,(1+i)\,(2+i)\,(1+2i)$	50	$16=2^2.\,2^2$	4	2	$4+i,\ 9+4i$	$5,\ 3+i,\ 8+4i$	10	5	1

m.	N (m).	Φ (m).	H.E.	No. of gens.	Gens. used.	The numbers ξ.	$d\,(\alpha^2+\beta^2)$.	d.	$-(\alpha\alpha'+\beta\beta'.)$
$6+4i=-i\,(1+i)^2\,(3+2i)$ $4+6i=-i\,(1+i)^2\,(2+3i)$	52	$24=2.\,2^2.\,3$	12	2	$15,\ 22+i$ $15,\ 6+i$	13, 14	26	2	5 21
$7+2i$ $2+7i$	53	$52=2^2.\,13$	52	1	3	..	53	..	23 30
$7+3i=-i\,(1+i)\,(2+5i)$ $3+7i=\ (1+i)\,(5+2i)$	58	$28=2^2.\,7$	28	1	3	29, 30	58	..	17 41
$6+5i$ $5+6i$	61	$60=2^2.\,3.\,5$	60	1	2	..	61	..	11 50
$8\ =\ i\,(1+i)^6$	64	$32=2.\,2^2.\,2^2$	4	3	$i,\ 1+2i,\ 3$	..	8	8	
$8+i\ =-i\,(1+2i)\,(3+2i)$ $1+8i=\ (2+i)\,(2+3i)$ $7+4i=-i\,(1+2i)\,(2+3i)$ $4+7i=\ (2+i)\,(3+2i)$	65	$48=2^2.\,2^2.\,3$	12	2	27, 2	26, 40	65	..	57 8 47 18
$8+2i=-i\,(1+i)^2\,(4+i)$ $2+8i=-i\,(1+i)^2\,(1+4i)$	68	$32=2.\,2^4$	16	2	$3,\ i$ $3,\ 26+i$	17, 18	34	2	13 21
$6+6i=-i\,(1+i)^3.\,3$	72	$32=2^2.\,2^3$	8	2	$2+i,\ i$	9, 4	12	6	1
$8+3i$ $3+8i$	73	$72=2^3.\,3^2$	72	1	5	..	73	..	46 27
$7+5i=-i\,(1+i)\,(1+6i)$ $5+7i=\ (1+i)\,(6+i)$	74	$36=2^2.\,3^2$	36	1	5	37, 38	74	..	43 31
$8+4i=-\ (1+i)^4\,(2+i)$ $4+8i=-\ (1+i)^4\,(1+2i)$	80	$32=2.\,2^2.\,2^2$	4	3	$17,\ 8+i,\ 5+2i$ $17,\ 3i,\ 17+2i$	5, 16	20	4	3 17
$9\ =\ 3^2$	81	$72=2^3.\,3.\,3$	24	2	$2+i,\ 4+3i$	..	9	9	
$9+i\ =-i\,(1+i)\,(4+5i)$ $1+9i=\ (1+i)\,(5+4i)$	82	$40=2^3.\,5$	40	1	7	41, 42	82	..	73 9
$9+2i=-i\,(2+i)\,(1+4i)$ $2+9i=\ (1+2i)\,(4+i)$ $7+6i=\ (2+i)\,(4+i)$ $6+7i=-i\,(1+2i)\,(1+4i)$	85	$64=2^2.\,2^4$	16	2	3, 52	51, 35	85	..	38 47 13 72
$8+5i$ $5+8i$	89	$88=2^3.\,11$	88	1	3	..	89	..	34 55
$9+3i=-i\,(1+i)\,(1+2i).\,3$ $3+9i=\ (1+i)\,(2+i).\,3$	90	$32=2^2.\,2^3$	8	2	$2+i,\ i$ $23+2i,\ 21+2i$	15, 6, 10	30	3	7 23
$9+4i$ $4+9i$	97	$96=2^5.\,3$	96	1	5	..	97	..	22 75
$7+7i=\ (1+i).\,7$	98	$48=2^4.\,3$	48	1	$2+i$	7. 8	14	7	1
$8+6i=-\ (1+i)^2\,(1+2i)^2$ $6+8i=-i\,(1+i)^2\,(2+i)^2$	100	$40=2.\,2^2.\,5$	20	2	$3,\ 44+i$ $3,\ 8+i$	25, 26	50	2	7 43
$10\ =-i\,(1+i)^2\,(2+i)\,(1+2i)$	100	$32=2.\,2^2.\,2^2$	4	3	$9+4i,\ 9+6i,\ 6+5i$	$5,\ 8+6i,\ 8+4i$	10	10	

$m = 2 + i \quad \mathrm{N}(m) = 5 \quad \Phi(m) = 4 = 2^2 \quad \mathrm{H.E} = 4 \quad x \equiv \mathrm{X} + 3\mathrm{Y} \pmod{5}.$

$m = 1 + 2i \quad \mathrm{N}(m) = 5 \quad \Phi(m) = 4 = 2^2 \quad \mathrm{H.E} = 4 \quad x \equiv \mathrm{X} + 2\mathrm{Y} \pmod{5}.$

Generator 2.

N	2	4	3	1
I	1	2	3	0

(4)

$m = 3 \quad \mathrm{N}(m) = 9 \quad \Phi(m) = 8 = 2^3 \quad \mathrm{H.E} = 8 \quad x \equiv \mathrm{X} \pmod{3} \quad y \equiv \mathrm{Y} \pmod{3}.$

Generator $1 + i$.

0	1
1	$1+i$
2	$2i$
3	$1+2i$
4	2
5	$2+2i$
6	i
7	$2+i$

(8)

i	6
$2i$	2
1	0
$1+i$	1
$1+2i$	3
2	4
$2+i$	7
$2+2i$	5

(8)

$m = 3 + i \;=\; -i(1 + i)(1 + 2i) \quad \mathrm{N}(m) = 10 \quad \Phi(m) = 4 = 2^2 \quad \mathrm{H.E} = 4$

$x \equiv \mathrm{X} + 7\mathrm{Y} \pmod{10}.$

$m = 1 + 3i = \quad (1 + i)(2 + i) \quad \mathrm{N}(m) = 10 \quad \Phi(m) = 4 = 2^2 \quad \mathrm{H.E} = 4$

$x \equiv \mathrm{X} + 3\mathrm{Y} \pmod{10}.$

Generator 3.

N	3	9	7	1
I	1	2	3	0

(4)

$m = 3 + 2i \quad \mathrm{N}(m) = 13 \quad \Phi(m) = 12 = 2^2.3 \quad \mathrm{H.E} = 12 \quad x \equiv \mathrm{X} + 5\mathrm{Y} \pmod{13}.$

$m = 2 + 3i \quad \mathrm{N}(m) = 13 \quad \Phi(m) = 12 = 2^2.3 \quad \mathrm{H.E} = 12 \quad x \equiv \mathrm{X} + 8\mathrm{Y} \pmod{13}.$

Generator 2.

I	0	1	2	3	4	5	6	7	8	9	10	11	(12)
N	1	2	4	8	3	6	12	11	9	5	10	7	

N	1	2	3	4	5	6	7	8	9	10	11	12	
I	0	1	4	2	9	5	11	3	8	10	7	6	(12)

$m = 4 + i \quad \mathrm{N}(m) = 17 \quad \Phi(m) = 16 = 2^4 \quad \mathrm{H.E} = 16 \quad x \equiv \mathrm{X} + 13\mathrm{Y} \pmod{17}.$

$m = 1 + 4i \quad \mathrm{N}(m) = 17 \quad \Phi(m) = 16 = 2^4 \quad \mathrm{H.E} = 16 \quad x \equiv \mathrm{X} + 4\mathrm{Y} \pmod{17}.$

Generator 3.

I	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	(16)
N	1	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	

N	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	
I	0	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8	(16)

$m = 3 + 3i = (1 + i)3 \quad \mathrm{N}(m) = 18 \quad \Phi(m) = 8 = 2^3 \quad \mathrm{H.E} = 8 \quad y \equiv \mathrm{Y} \pmod{3}$

$x \equiv \mathrm{X} + 3(\mathrm{Y} - y) \pmod{6}.$

Generator $1 + 2i$.

0	1
1	$1+2i$
2	i
3	$4+i$
4	5
5	$2+i$
6	$3+2i$
7	$5+2i$

(8)

i	2
1	0
$1+2i$	1
$2+i$	5
$3+2i$	6
$4+i$	3
5	4
$5+2i$	7

(8)

$$m = 4 + 2i = -i(1+i)^2(2+i) \quad \mathrm{N}(m) = 20 \quad \Phi(m) = 8 = 2.\,2^2 \quad \mathrm{H.\,E.} = 4$$

$$y \equiv \mathrm{Y} \pmod{2} \quad x = \mathrm{X} + 3(\mathrm{Y} - y) \pmod{10}.$$

Generators 7, $8+i$.

0	0	1
0	1	$8+i$
1	0	7
1	1	$4+i$
2	0	9
2	1	$6+i$
3	0	3
3	1	i
(4)	(2)	

i	3	1
1	0	0
3	3	0
$4+i$	1	1
$6+i$	2	1
7	1	0
$8+i$	0	1
9	2	0
	(4)	(2)

$$m = 2 + 4i = -i(1+i)^2(1+2i) \quad \mathrm{N}(m) = 20 \quad \Phi(m) = 8 = 2.\,2^2 \quad \mathrm{H.\,E.} = 4$$

$$y \equiv \mathrm{Y} \pmod{2} \quad x \equiv \mathrm{X} + 7(\mathrm{Y} - y) \pmod{10}.$$

Generators 7, $4+i$.

0	0	1
0	1	$4+i$
1	0	7
1	1	i
2	0	9
2	1	$2+i$
3	0	3
3	1	$6+i$
(4)	(2)	

i	1	1
1	0	0
$2+i$	2	1
3	3	0
$4+i$	0	1
$6+i$	3	1
7	1	0
9	2	0
	(4)	(2)

$$m = 5 = -i(2+i)(1+2i) \quad \mathrm{N}(m) = 25 \quad \Phi(m) = 16 = 2^2.\,2^2 \quad \mathrm{H.\,E.} = 4$$

$$x \equiv \mathrm{X} \pmod{5} \quad y \equiv \mathrm{Y} \pmod{5}.$$

Generators $4+i$, $4+4i$.

0	0	1
0	1	$4+4i$
0	2	$2i$
0	3	$2+3i$
1	0	$4+i$
1	1	2
1	2	$3+3i$
1	3	$4i$
2	0	$3i$
2	1	$3+2i$
2	2	4
2	3	$1+i$
3	0	$2+2i$
3	1	i
3	2	$1+4i$
3	3	3
(4)	(4)	

i	3	1
$2i$	0	2
$3i$	2	0
$4i$	1	3
1	0	0
$1+i$	2	3
$1+4i$	3	2
2	1	1
$2+2i$	3	0
$2+3i$	0	3
3	3	3
$3+2i$	2	1
$3+3i$	1	2
4	2	2
$4+i$	1	0
$4+4i$	0	1
	(4)	(4)

$$m = 4 + 3i = -i(1+2i)^2 \quad \mathrm{N}(m) = 25 \quad \Phi(m) = 20 = 2^2 . 5 \quad \text{H. E.} = 20$$
$$x \equiv \mathrm{X} + 7\mathrm{Y} \pmod{25}.$$

$$m = 3 + 4i = \quad (2+i)^2 \quad \mathrm{N}(m) = 25 \quad \Phi(m) = 20 = 2^2 . 5 \quad \text{H. E.} = 20$$
$$x \equiv \mathrm{X} + 18\mathrm{Y} \pmod{25}.$$

Generator 2.

I	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	(20)
N	1	2	4	8	16	7	14	3	6	12	24	23	21	17	9	18	11	22	19	13	

N	1	2	3	4	6	7	8	9	11	12	13	14	16	17	18	19	21	22	23	24	
I	0	1	7	2	8	5	3	14	16	9	19	6	4	13	15	18	12	17	11	10	(20)

$$m = 5 + i = -i(1+i)(2+3i) \quad \mathrm{N}(m) = 26 \quad \Phi(m) = 12 = 2^2 . 3 \quad \text{H. E.} = 12$$
$$x \equiv \mathrm{X} + 21\mathrm{Y} \pmod{26}.$$

$$m = 1 + 5i = \quad (1+i)(3+2i) \quad \mathrm{N}(m) = 26 \quad \Phi(m) = 12 = 2^2 . 3 \quad \text{H. E.} = 12$$
$$x \equiv \mathrm{X} + 5\mathrm{Y} \pmod{26}.$$

Generator 7.

I	0	1	2	3	4	5	6	7	8	9	10	11	(12)
N	1	7	23	5	9	11	25	19	3	21	17	15	

N	1	3	5	7	9	11	15	17	19	21	23	25	
I	0	8	3	1	4	5	11	10	7	9	2	6	(12)

$m = 5 + 2i \quad N(m) = 29 \quad \Phi(m) = 28 = 2^2.\,7 \quad \text{H. E.} = 28 \quad x \equiv X + 12Y \pmod{29}.$

$m = 2 + 5i \quad N(m) = 29 \quad \Phi(m) = 28 = 2^2.\,7 \quad \text{H. E.} = 28 \quad x \equiv X + 17Y \pmod{29}.$

Generator 2.

I	0	1	2	3	4	5	6	7	8	9	10	11	12	13	(28)
N	1	2	4	8	16	3	6	12	24	19	9	18	7	14	
I	14	15	16	17	18	19	20	21	22	23	24	25	26	27	(28)
N	28	27	25	21	13	26	23	17	5	10	20	11	22	15	

N	1	2	3	4	5	6	7	8	9	10	11	12	13	14	
I	0	1	5	2	22	6	12	3	10	23	25	7	18	13	(28)
N	15	16	17	18	19	20	21	22	23	24	25	26	27	28	
I	27	4	21	11	9	24	17	26	20	8	16	19	15	14	(28)

$m = 5 + 3i = -i(1+i)(1+4i) \quad N(m) = 34 \quad \Phi(m) = 16 = 2^4 \quad \text{H. E.} = 16$

$x \equiv X + 21Y \pmod{34}.$

$m = 3 + 5i = \quad (1+i)(4+i) \quad N(m) = 34 \quad \Phi(m) = 16 = 2^4 \quad \text{H. E.} = 16$

$x \equiv X + 13Y \pmod{34}.$

Generator 3.

I	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	(16)
N	1	3	9	27	13	5	15	11	33	31	25	7	21	29	19	23	

N	1	3	5	7	9	11	13	15	19	21	23	25	27	29	31	33	
I	0	1	5	11	2	7	4	6	14	12	15	10	3	13	9	8	(16)

$$m = 6 = -i(1+i)^2.\ 3 \quad \mathrm{N}(m) = 36 \quad \Phi(m) = 16 = 2.\ 2^3 \quad \mathrm{H.\,E.} = 8$$

$$x \equiv \mathrm{X}\ (\mathrm{mod}\ 6) \quad y \equiv \mathrm{Y}\ (\mathrm{mod}\ 6).$$

Generators $1+4i$, $4+3i$.

0	0	1
0	1	$4+3i$
1	0	$1+4i$
1	1	$4+i$
2	0	$3+2i$
2	1	$5i$
3	0	$1+2i$
3	1	$4+5i$
4	0	5
4	1	$2+3i$
5	0	$5+2i$
5	1	$2+5i$
6	0	$3+4i$
6	1	i
7	0	$5+4i$
7	1	$2+i$
(8)	(2)	

i	6	1
$5i$	2	1
1	0	0
$1+2i$	3	0
$1+4i$	1	0
$2+i$	7	1
$2+3i$	4	1
$2+5i$	5	1
$3+2i$	2	0
$3+4i$	6	0
$4+i$	1	1
$4+3i$	0	1
$4+5i$	3	1
5	4	0
$5+2i$	5	0
$5+4i$	7	0
	(8)	(2)

$$m = 6+i \quad \mathrm{N}(m) = 37 \quad \Phi(m) = 36 = 2^2.\ 3^2 \quad \mathrm{H.\,E.} = 36 \quad x \equiv \mathrm{X} + 31\mathrm{Y}\ (\mathrm{mod}\ 37).$$

$$m = 1+6i \quad \mathrm{N}(m) = 37 \quad \Phi(m) = 36 = 2^2.\ 3^2 \quad \mathrm{H.\,E.} = 36 \quad x \equiv \mathrm{X} + 6\mathrm{Y}\ (\mathrm{mod}\ 37).$$

Generator 2.

I	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	(36)
N	1	2	4	8	16	32	27	17	34	31	25	13	26	15	30	23	9	18	
I	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	(36)
N	36	35	33	29	21	5	10	20	3	6	12	24	11	22	7	14	28	19	

N	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	
I	0	1	26	2	23	27	32	3	16	24	30	28	11	33	13	4	7	17	(36)
N	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	
I	35	25	22	31	15	29	10	12	6	34	21	14	9	5	20	8	19	18	(36)

$$m = 6 + 2i = -(1 + i)^3 (1 + 2i) \quad \mathrm{N}(m) = 40 \quad \Phi(m) = 16 = 2^2 . 2^2 \quad \text{H. E.} = 4.$$

$$y \equiv \mathrm{Y} \pmod 2 \quad x \equiv \mathrm{X} + 7(\mathrm{Y} - y) \pmod{20}.$$

Generators 3, i.

0	0	1
0	1	i
0	2	19
0	3	$6+i$
1	0	3
1	1	$14+i$
1	2	17
1	3	$12+i$
2	0	9
2	1	$16+i$
2	2	11
2	3	$10+i$
3	0	7
3	1	$2+i$
3	2	13
3	3	$4+i$
(4)	(4)	

i	0	1
1	0	0
$2+i$	3	1
3	1	0
$4+i$	3	3
$6+i$	0	3
7	3	0
9	2	0
$10+i$	2	3
11	2	2
$12+i$	1	3
13	3	2
$14+i$	1	1
$16+i$	2	1
17	1	2
19	0	2
	(4)	(4)

$$m = 2 + 6i = -i(1 + i)^3 (2 + i) \quad \mathrm{N}(m) = 40 \quad \Phi(m) = 16 = 2^2 . 2 \quad \text{H. E.} = 4.$$

$$y \equiv \mathrm{Y} \pmod 2 \quad x \equiv \mathrm{X} + 13(\mathrm{Y} - y) \pmod{20}.$$

Generators 3, $14 + i$.

0	0	1
0	1	$14+i$
0	2	19
0	3	i
1	0	3
1	1	$8+i$
1	2	17
1	3	$6+i$
2	0	9
2	1	$10+i$
2	2	11
2	3	$4+i$
3	0	7
3	1	$16+i$
3	2	13
3	3	$18+i$
(4)	(4)	

i	0	3
1	0	0
3	1	0
$4+i$	2	3
$6+i$	1	3
7	3	0
$8+i$	1	1
9	2	0
$10+i$	2	1
11	2	2
13	3	2
$14+i$	0	1
$16+i$	3	1
17	1	2
$18+i$	3	3
19	0	2
	(4)	(4)

$m = 5 + 4i \quad \mathrm{N}(m) = 41 \quad \Phi(m) = 40 = 2^3 .\ 5 \quad \mathrm{H.\,E.} = 40 \quad x \equiv \mathrm{X} + 9\mathrm{Y} \quad (\mathrm{mod}\ 41).$

$m = 4 + 5i \quad \mathrm{N}(m) = 41 \quad \Phi(m) = 40 = 2^3 .\ 5 \quad \mathrm{H.\,E.} = 40 \quad x \equiv \mathrm{X} + 32\mathrm{Y} \quad (\mathrm{mod}\ 41).$

Generator 6.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	
N	1	6	36	11	25	27	39	29	10	19	32	28	4	24	21	3	18	26	33	34	(40)
I	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	
N	40	35	5	30	16	14	2	12	31	22	9	13	37	17	20	38	23	15	8	7	(40)

I	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	
N	0	26	15	12	22	1	39	38	30	8	3	27	31	25	37	24	33	16	9	34	(40)
I	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	
N	14	29	36	13	4	17	5	11	7	23	28	10	18	19	21	2	32	35	6	20	(40)

$$m = 6 + 3i = (2 + i)\,3 \qquad \mathrm{N}(m) = 45 \qquad \Phi(m) = 32 = 2^2 . \, 2^3$$

$$\mathrm{H.\,E.} = 8 \qquad y \equiv \mathrm{Y} \pmod{3} \qquad x \equiv \mathrm{X} + 3(\mathrm{Y} - y) \pmod{15}.$$

Generators $1 + i$, i.

0	0	1
0	1	i
0	2	14
0	3	$6+2i$
1	0	$1+i$
1	1	$14+i$
1	2	$5+2i$
1	3	$7+2i$
2	0	$2i$
2	1	13
2	2	$6+i$
2	3	2
3	0	$13+2i$
3	1	$4+i$
3	2	$8+i$
3	3	$2+2i$
4	0	11
4	1	$12+2i$
4	2	4
4	3	$9+i$
5	0	$8+2i$
5	1	$1+2i$
5	2	$13+i$
5	3	$5+i$
6	0	$3+i$
6	1	8
6	2	$3+2i$
6	3	7
7	0	$11+i$
7	1	$11+2i$
7	2	$10+2i$
7	3	$10+i$
(8)	(4)	

i	0	1
$2i$	2	0
1	0	0
$1+i$	1	0
$1+2i$	5	1
2	2	3
$2+2i$	3	3
$3+i$	6	0
$3+2i$	6	2
4	4	2
$4+i$	3	1
$5+i$	5	3
$5+2i$	1	2
$6+i$	2	2
$6+2i$	0	3
7	6	3
$7+2i$	1	3
8	6	1
$8+i$	3	2
$8+2i$	5	0
$9+i$	4	3
$10+i$	7	3
$10+2i$	7	2
11	4	0
$11+i$	7	0
$11+2i$	7	1
$12+2i$	4	1
13	2	1
$13+i$	5	2
$13+2i$	3	0
14	0	2
$14+i$	1	1
	(8)	(4)

$$m = 3 + 6i = (1 + 2i)\,3 \qquad \mathrm{N}(m) = 45 \qquad \Phi(m) = 32 = 2^2 .\, 2^3$$

$$\text{H. E.} = 8 \qquad y \equiv \mathrm{Y} \pmod{3} \qquad x \equiv \mathrm{X} + 12(\mathrm{Y} - y) \pmod{15}.$$

Generators $10 + 2i$, $9 + 2i$.

0	0	1
0	1	$9+2i$
0	2	14
0	3	i
1	0	$10+2i$
1	1	$8+2i$
1	2	$14+i$
1	3	$1+i$
2	0	$9+i$
2	1	13
2	2	$2i$
2	3	2
3	0	$7+i$
3	1	$13+2i$
3	2	$2+2i$
3	3	$11+i$
4	0	11
4	1	$6+i$
4	2	4
4	3	$3+2i$
5	0	$2+i$
5	1	$10+i$
5	2	$7+2i$
5	3	$14+2i$
6	0	$12+2i$
6	1	8
6	2	$12+i$
6	3	7
7	0	$5+2i$
7	1	$5+i$
7	2	$4+i$
7	3	$4+2i$
(8)	(4)	

i	0	3
$2i$	2	2
1	0	0
$1+i$	1	3
2	2	3
$2+i$	5	0
$2+2i$	3	2
$3+2i$	4	3
4	4	2
$4+i$	7	2
$4+2i$	7	3
$5+i$	7	1
$5+2i$	7	0
$6+i$	4	1
7	6	3
$7+i$	3	0
$7+2i$	5	2
8	6	1
$8+2i$	1	1
$9+i$	2	0
$9+2i$	0	1
$10+i$	5	1
$10+2i$	1	0
11	4	0
$11+i$	3	3
$12+i$	6	2
$12+2i$	6	0
13	2	1
$13+2i$	3	1
14	0	2
$14+i$	1	2
$14+2i$	5	3
	(8)	(4)

$m = 7 \quad \mathrm{N}(7) = 49 \quad \Phi(7) = 48 = 2^4.3. \quad \mathrm{H.\,E.} = 48. \quad x \equiv \mathrm{X} \pmod{7}$
$y \equiv \mathrm{Y} \pmod{7}.$

Generator $2 + i$.

0	1
1	$2+i$
2	$3+4i$
3	$2+4i$
4	$3i$
5	$4+6i$
6	$2+2i$
7	$2+6i$
8	5
9	$3+5i$
10	$1+6i$
11	$3+6i$
12	i
13	$6+2i$
14	$3+3i$
15	$3+2i$
16	4
17	$1+4i$
18	$5+2i$
19	$1+2i$
20	$5i$
21	$2+3i$
22	$1+i$
23	$1+3i$

(48)

24	6
25	$5+6i$
26	$4+3i$
27	$5+3i$
28	$4i$
29	$3+i$
30	$5+5i$
31	$5+i$
32	2
33	$4+2i$
34	$6+i$
35	$4+i$
36	$6i$
37	$1+5i$
38	$4+4i$
39	$4+5i$
40	3
41	$6+3i$
42	$2+5i$
43	$6+5i$
44	$2i$
45	$5+4i$
46	$6+6i$
47	$6+4i$

(48)

i	12
$2i$	44
$3i$	4
$4i$	28
$5i$	20
$6i$	36
1	0
$1+i$	22
$1+2i$	19
$1+3i$	23
$1+4i$	17
$1+5i$	37
$1+6i$	10
2	32
$2+i$	1
$2+2i$	6
$2+3i$	21
$2+4i$	3
$2+5i$	42
$2+6i$	7
3	40
$3+i$	29
$3+2i$	15
$3+3i$	14

(48)

$3+4i$	2
$3+5i$	9
$3+6i$	11
4	16
$4+i$	35
$4+2i$	33
$4+3i$	26
$4+4i$	38
$4+5i$	39
$4+6i$	5
5	8
$5+i$	31
$5+2i$	18
$5+3i$	27
$5+4i$	45
$5+5i$	30
$5+6i$	25
6	24
$6+i$	34
$6+2i$	13
$6+3i$	41
$6+4i$	47
$6+5i$	43
$6+6i$	46

(48)

$m = 7 + i = -i(1+i)(2+i)^2 \quad \mathrm{N}(m) = 50 \quad \Phi(m) = 20 = 2^2.5 \quad \mathrm{H.\,E.} = 20$
$x \equiv \mathrm{X} + 43\mathrm{Y} \pmod{50}.$

$m = 1 + 7i = -i(1+i)(1+2i)^2 \quad \mathrm{N}(m) = 50 \quad \Phi(m) = 20 = 2^2.5 \quad \mathrm{H.\,E.} = 20$
$x \equiv \mathrm{X} + 7\mathrm{Y} \pmod{50}.$

Generator 3.

I	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	(20)
N	1	3	9	27	31	43	29	37	11	33	49	47	41	23	19	7	21	13	39	17	

N	1	3	7	9	11	13	17	19	21	23	27	29	31	33	37	39	41	43	47	49	
I	0	1	15	2	8	17	19	14	16	13	3	6	4	9	7	18	12	5	11	10	(20)

$$m = 5 + 5i = -i(1+i)(2+i)(1+2i) \quad \mathrm{N}(m) = 50 \quad \Phi(m) = 16 = 2^2 . 2^2$$

$$\mathrm{H.E.} = 4 \quad y \equiv \mathrm{Y} \pmod{5} \quad x \equiv \mathrm{X} + \mathrm{Y} - y \pmod{10}.$$

Generators $4 + i$, $9 + 4i$.

0	0	1
0	1	$9+4i$
0	2	$5+2i$
0	3	$2+3i$
1	0	$4+i$
1	1	7
1	2	$8+3i$
1	3	$5+4i$
2	0	$3i$
2	1	$3+2i$
2	2	9
2	3	$6+i$
3	0	$7+2i$
3	1	i
3	2	$1+4i$
3	3	3
(4)	(4)	

i	3	1
$3i$	2	0
1	0	0
$1+4i$	3	2
$2+3i$	0	3
3	3	3
$3+2i$	2	1
$4+i$	1	0
$5+2i$	0	2
$5+4i$	1	3
$6+i$	2	3
7	1	1
$7+2i$	3	0
$8+3i$	1	2
9	2	2
$9+4i$	0	1
	(4)	(4)

$$m = 6 + 4i = -i(1+i)^2(3+2i) \quad \mathrm{N}(m) = 52 \quad \Phi(m) = 24 = 2 . 2^2 . 3 \quad \mathrm{H.E.} = 12$$

$$y \equiv \mathrm{Y} \pmod{2} \quad x \equiv \mathrm{X} + 5(\mathrm{Y} - y) \pmod{26}.$$

Generators 15, $22 + i$.

0	0	1
0	1	$22+i$
1	0	15
1	1	$10+i$
2	0	17
2	1	$12+i$
3	0	21
3	1	$16+i$
4	0	3
4	1	$24+i$
5	0	19
5	1	$14+i$
6	0	25
6	1	$20+i$
7	0	11
7	1	$6+i$
8	0	9
8	1	$4+i$
9	0	5
9	1	i
10	0	23
10	1	$18+i$
11	0	7
11	1	$2+i$
(12)	(2)	

i	9	1
1	0	0
$2+i$	11	1
3	4	0
$4+i$	8	1
5	9	0
$6+i$	7	1
7	11	0
9	8	0
$10+i$	1	1
11	7	0
$12+i$	2	1
$14+i$	5	1
15	1	0
$16+i$	3	1
17	2	0
$18+i$	10	1
19	5	0
$20+i$	6	1
21	3	0
$22+i$	0	1
23	10	0
$24+i$	4	1
25	6	0
	(12)	(2)

$m = 4 + 6i = -i\,(1+i)^2\,(2+3i)$ $\quad \mathrm{N}(m) = 52 \quad \Phi(m) = 24 = 2.\,2^2.\,3 \quad$ H. E. $= 12$

$y \equiv \mathrm{Y} \pmod{2} \quad x \equiv \mathrm{X} + 21\,(\mathrm{Y} - y) \pmod{26}.$

Generators 15, $6 + i$.

0	0	1
0	1	$6+i$
1	0	15
1	1	$20+i$
2	0	17
2	1	$22+i$
3	0	21
3	1	i
4	0	3
4	1	$8+i$
5	0	19
5	1	$24+i$
6	0	25
6	1	$4+i$
7	0	11
7	1	$16+i$
8	0	9
8	1	$14+i$
9	0	5
9	1	$10+i$
10	0	23
10	1	$2+i$
11	0	7
11	1	$12+i$
(12)	(2)	

i	3	1
1	0	0
$2+i$	10	1
3	4	0
$4+i$	6	1
5	9	0
$6+i$	0	1
7	11	0
$8+i$	4	1
9	8	0
$10+i$	9	1
11	7	0
$12+i$	11	1
$14+i$	8	1
15	1	0
$16+i$	7	1
17	2	0
19	5	0
$20+i$	1	1
21	3	0
$22+i$	2	1
23	10	0
$24+i$	5	1
25	6	0
	(12)	(2)

$m = 7 + 2i \quad \mathrm{N}(m) = 53 \quad \Phi(m) = 52 = 2^2.\,13 \quad$ H. E. $= 52 \quad x \equiv \mathrm{X} + 23\mathrm{Y} \pmod{53}.$

$m = 2 + 7i \quad \mathrm{N}(m) = 53 \quad \Phi(m) = 52 = 2^2.\,13 \quad$ H. E. $= 52 \quad x \equiv \mathrm{X} + 30\mathrm{Y} \pmod{53}.$

Generator 3.

I	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	(52)
N	1	3	9	27	28	31	40	14	42	20	7	21	10	30	37	5	15	45	29	
I	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36		(52)
N	34	49	41	17	51	47	35	52	50	44	26	25	22	13	39	11	33	46		
I	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51					(52)
N	32	43	23	16	48	38	8	24	19	4	12	36	2	6	13					

N	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	
I	0	49	1	46	15	50	10	43	2	12	34	47	32	7	16	40	22	51	45	(52)
N	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37		
I	9	11	31	39	44	30	29	3	4	18	13	5	37	35	19	25	48	14		(52)
N	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52					
I	42	33	6	21	8	38	28	17	36	24	41	20	27	23	26					(52)

$m = 7 + 3i = -i(1+i)(2+5i)$ $\mathrm{N}(m) = 58$ $\Phi(m) = 28 = 2^2.7$ H. E. $= 28$

$$x \equiv \mathrm{X} + 17\mathrm{Y} \pmod{58}.$$

$m = 3 + 7i = (1+i)(5+2i)$ $\mathrm{N}(m) = 58$ $\Phi(m) = 28 = 2^2.7$ H. E. $= 28$

$$x \equiv \mathrm{X} + 41\mathrm{Y} \pmod{58}.$$

Generator 3.

I	0	1	2	3	4	5	6	7	8	9	10	11	12	13	
N	1	3	9	27	23	11	33	41	7	21	5	15	45	19	(28)
I	14	15	16	17	18	19	20	21	22	23	24	25	26	27	
N	57	55	49	31	35	47	25	17	51	37	53	43	13	39	(28)

N	1	3	5	7	9	11	13	15	17	19	21	23	25	27	
I	0	1	10	8	2	5	26	11	21	13	9	4	20	3	(28)
N	31	33	35	37	39	41	43	45	47	49	51	53	55	57	
I	17	6	18	23	27	7	25	12	19	16	22	24	15	14	(28)

$m = 6 + 5i \quad \mathrm{N}(m) = 61 \quad \Phi(m) = 60 = 2^2.3.5 \quad \mathrm{H.\ E.} = 60 \quad x \equiv \mathrm{X} + 11\mathrm{Y} \pmod{61}.$

$m = 5 + 6i \quad \mathrm{N}(m) = 61 \quad \Phi(m) = 60 = 2^2.3.5 \quad \mathrm{H.\ E.} = 60 \quad x \equiv \mathrm{X} + 50\mathrm{Y} \pmod{61}.$

Generator 2.

I	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	(60)
N	1	2	4	8	16	32	3	6	12	24	48	35	9	18	36	11	22	44	27	54	
I	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	(60)
N	47	33	5	10	20	40	19	38	15	30	60	59	57	53	45	29	58	55	49	37	
I	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	(60)
N	13	26	52	43	25	50	39	17	34	7	14	28	56	51	41	21	42	23	46	31	

N	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	
I	0	1	6	2	22	7	49	3	12	23	15	8	40	50	28	4	47	13	26	24	(60)
N	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	
I	55	16	57	9	44	41	18	51	35	29	59	5	21	48	11	14	39	27	46	25	(60)
N	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	
I	54	56	43	17	34	58	20	10	38	45	53	42	33	19	37	52	32	36	31	30	(60)

$m = 8 + i = -i(1 + 2i)(3 + 2i) \quad \mathrm{N}(m) = 65 \quad \Phi(m) = 48 = 2^2 . 2^2 . 3$

H. E. $= 12 \quad x \equiv \mathrm{X} + 57\mathrm{Y} \pmod{65}$.

$m = 1 + 8i = (2 + i)(2 + 3i) \quad \mathrm{N}(m) = 65 \quad \Phi(m) = 48 = 2^2 . 2^2 . 3$

H. E. $= 12 \quad x \equiv \mathrm{X} + 8\mathrm{Y} \pmod{65}$.

$m = 7 + 4i = -i(1 + 2i)(2 + 3i) \quad \mathrm{N}(m) = 65 \quad \Phi(m) = 48 = 2^2 . 2^2 . 3$

H. E. $= 12 \quad x \equiv \mathrm{X} + 47\mathrm{Y} \pmod{65}$.

$m = 4 + 7i = (2 + i)(3 + 2i) \quad \mathrm{N}(m) = 65 \quad \Phi(m) = 48 = 2^2 . 2^2 . 3$

H. E. $= 12 \quad x \equiv \mathrm{X} + 18\mathrm{Y} \pmod{65}$.

Generators 27, 2.

0	0	0	0	1	1	1	1	2	2	2	2	3	3	3	3	4	4	4	4	5	5	5	5	(12)
0	1	2	3	0	1	2	3	0	1	2	3	0	1	2	3	0	1	2	3	0	1	2	3	(4)
1	27	14	53	2	54	28	41	4	43	56	17	8	21	47	34	16	42	29	3	32	19	58	6	
6	6	6	6	7	7	7	7	8	8	8	8	9	9	9	9	10	10	10	10	11	11	11	11	(12)
0	1	2	3	0	1	2	3	0	1	2	3	0	1	2	3	0	1	2	3	0	1	2	3	(4)
64	38	51	12	63	11	37	24	61	22	9	48	57	44	18	31	49	23	36	62	33	46	7	59	

1	2	3	4	6	7	8	9	11	12	14	16	17	18	19	21	22	23	24	27	28	29	31	32	
0	1	4	2	5	11	3	8	7	6	0	4	2	9	5	3	8	10	7	0	1	4	9	5	(12)
0	0	3	0	3	2	0	2	1	3	2	0	3	2	1	1	1	1	3	1	2	2	3	0	(4)
33	34	36	37	38	41	42	43	44	46	47	48	49	51	53	54	56	57	58	59	61	62	63	64	
11	3	10	7	6	1	4	2	9	11	3	8	10	6	0	1	2	9	5	11	8	10	7	6	(12)
0	3	2	2	1	3	1	1	1	1	2	3	0	2	3	1	2	0	2	3	0	3	0	0	(4)

$$m = 8 + 2i = -i(1+i)^2(4+i) \quad N(m) = 68 \quad \Phi(m) = 32 = 2.2^4 \quad \text{H. E.} = 16$$

$$y \equiv Y \pmod 2 \quad x \equiv X + 13(Y - y) \pmod{34}.$$

Generators 3, i.

(16)	(2)	
0	0	1
0	1	i
1	0	3
1	1	$26+i$
2	0	9
2	1	$2+i$
3	0	27
3	1	$32+i$
4	0	13
4	1	$20+i$
5	0	5
5	1	$18+i$
6	0	15
6	1	$12+i$
7	0	11
7	1	$28+i$
8	0	33
8	1	$8+i$
9	0	31
9	1	$16+i$
10	0	25
10	1	$6+i$
11	0	7
11	1	$10+i$
12	0	21
12	1	$22+i$
13	0	29
13	1	$24+i$
14	0	19
14	1	$30+i$
15	0	23
15	1	$14+i$

	(16)	(2)
i	0	1
1	0	0
$2+i$	2	1
3	1	0
5	5	0
$6+i$	10	1
7	11	0
$8+i$	8	1
9	2	0
$10+i$	11	1
11	7	0
$12+i$	6	1
13	4	0
$14+i$	15	1
15	6	0
$16+i$	9	1
$18+i$	5	1
19	14	0
$20+i$	4	1
21	12	0
$22+i$	12	1
23	15	0
$24+i$	13	1
25	10	0
$26+i$	1	1
27	3	0
$28+i$	7	1
29	13	0
$30+i$	14	1
31	9	0
$32+i$	3	1
33	8	0

$$m = 2 + 8i = -i(1+i)^2(1+4i) \quad \mathrm{N}(m) = 68 \quad \Phi(m) = 32 = 2.\,2^4 \quad \text{H. E.} = 16$$

$$y \equiv \mathrm{Y} \pmod{2} \quad x \equiv \mathrm{X} + 21(\mathrm{Y} - y) \pmod{34}.$$

Generators 3, 26 + i.

0	0	1
0	1	26+i
1	0	3
1	1	18+i
2	0	9
2	1	28+i
3	0	27
3	1	24+i
4	0	13
4	1	12+i
5	0	5
5	1	10+i
6	0	15
6	1	4+i
7	0	11
7	1	20+i
8	0	33
8	1	i
9	0	31
9	1	8+i
10	0	25
10	1	32+i
11	0	7
11	1	2+i
12	0	21
12	1	14+i
13	0	29
13	1	16+i
14	0	19
14	1	22+i
15	0	23
15	1	6+i
(16)	(2)	

i	8	1
1	0	0
2+i	11	1
3	1	0
4+i	6	1
5	5	0
6+i	15	1
7	11	0
8+i	9	1
9	2	0
10+i	5	1
11	7	0
12+i	4	1
13	4	0
14+i	12	1
15	6	0
16+i	13	1
18+i	1	1
19	14	0
20+i	7	1
21	12	0
22+i	14	1
23	15	0
24+i	3	1
25	10	0
26+i	0	1
27	3	0
28+i	2	1
29	13	0
31	9	0
32 + i	10	1
33	8	0
	(16)	(2)

$$m = 6 + 6i = -i(1+i)^3 . 3 \quad \mathrm{N}(m) = 72 \quad \Phi(m) = 32 = 2^2 . 2^3 \quad \mathrm{H.\,E.} = 8$$

$$y \equiv \mathrm{Y} \pmod{6} \quad x \equiv \mathrm{X} + \mathrm{Y} - y \pmod{12}.$$

Generators $2 + i$, i.

0	0	1
0	1	i
0	2	11
0	3	$6+5i$
1	0	$2+i$
1	1	$11+2i$
1	2	$4+5i$
1	3	$7+4i$
2	0	$3+4i$
2	1	$8+3i$
2	2	$3+2i$
2	3	$10+3i$
3	0	$8+5i$
3	1	$1+2i$
3	2	$10+i$
3	3	$5+4i$
4	0	5
4	1	$5i$
4	2	7
4	3	$6+i$
5	0	$10+5i$
5	1	$1+4i$
5	2	$8+i$
5	3	$5+2i$
6	0	$9+2i$
6	1	$4+3i$
6	2	$9+4i$
6	3	$2+3i$
7	0	$4+i$
7	1	$11+4i$
7	2	$2+5i$
7	3	$7+2i$
(8)	(4)	

i	0	1
$5i$	4	1
1	0	0
$1+2i$	3	1
$1+4i$	5	1
$2+i$	1	0
$2+3i$	6	3
$2+5i$	7	2
$3+2i$	2	2
$3+4i$	2	0
$4+i$	7	0
$4+3i$	6	1
$4+5i$	1	2
5	4	0
$5+2i$	5	3
$5+4i$	3	3
$6+i$	4	3
$6+5i$	0	3
7	4	2
$7+2i$	7	3
$7+4i$	1	3
$8+i$	5	2
$8+3i$	2	1
$8+5i$	3	0
$9+2i$	6	0
$9+4i$	6	2
$10+i$	3	2
$10+3i$	2	3
$10+5i$	5	0
11	0	2
$11+2i$	1	1
$11+4i$	7	1
	(8)	(4)

$m = 8 + 3i$ $\quad N(m) = 73 \quad \Phi(m) = 72 = 2^3 . 3^2 \quad$ H. E. $= 72 \quad x \equiv X + 46Y \pmod{73}$

$m = 3 + 8i$ $\quad N(m) = 73 \quad \Phi(m) = 72 = 2^3 . 3^2 \quad$ H. E. $= 72 \quad x \equiv X + 27Y \pmod{73}$

Generator 5.

I	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	(72)
N	1	5	25	52	41	59	3	15	2	10	50	31	9	45	6	30	4	20	
I	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	(72)
N	27	62	18	17	12	60	8	40	54	51	36	34	24	47	16	7	35	29	
I	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	(72)
N	72	68	48	21	32	14	70	58	71	63	23	42	64	28	67	43	69	53	
I	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	(72)
N	46	11	55	56	61	13	65	33	19	22	37	39	49	26	57	66	38	44	

N	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	
I	0	8	6	16	1	14	33	24	12	9	55	22	59	41	7	32	21	20	(72)
N	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	
I	62	17	39	63	46	30	2	67	18	49	35	15	11	40	61	29	34	28	(72)
N	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	
I	64	70	65	25	4	47	51	71	13	54	31	38	66	10	27	3	53	26	(72)
N	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	
I	56	57	68	43	5	23	58	19	45	48	60	69	50	37	52	42	44	36	(72)

$$m = 7 + 5i = -i(1+i)(1+6i) \quad \mathrm{N}(m) = 74 \quad \Phi(m) = 36 = 2^2 . 3^2 \quad \mathrm{H.E.} = 36$$

$$x \equiv \mathrm{X} + 43\mathrm{Y} \pmod{74}$$

$$m = 5 + 7i = \quad (1+i)(6+i) \quad \mathrm{N}(m) = 74 \quad \Phi(m) = 36 = 2^2 . 3^2 \quad \mathrm{H.E.} = 36$$

$$x \equiv \mathrm{X} + 31\mathrm{Y} \pmod{74}.$$

Generator 5.

I	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	(36)
N	1	5	25	51	33	17	11	55	53	43	67	39	47	13	65	29	71	59	
I	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	(36)
N	73	69	49	23	41	57	63	19	21	31	7	35	27	61	9	45	3	15	

N	1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	
I	0	34	1	28	32	6	13	35	5	25	26	21	2	30	15	27	4	29	(36)
N	39	41	43	45	47	49	51	53	55	57	59	61	63	65	67	69	71	73	
I	11	22	9	33	12	20	3	8	7	23	17	31	24	14	10	19	16	18	(36

$$m = 8 + 4i = -(1+i)^4(2+i) \quad \mathrm{N}(m) = 80 \quad \Phi(m) = 32 = 2.2^2.2^2 \quad \mathrm{H.E.} = 4$$

$$y \equiv \mathrm{Y} \pmod{4} \quad x \equiv \mathrm{X} + 3(\mathrm{Y} - y) \pmod{20}.$$

Generators 17, $8 + i$, $5 + 2i$.

0	0	0	1
0	0	1	$5+2i$
0	1	0	$8+i$
0	1	1	$18+i$
0	2	0	11
0	2	1	$15+2i$
0	3	0	$12+3i$
0	3	1	$2+3i$
1	0	0	17
1	0	1	$1+2i$
1	1	0	$4+i$
1	1	1	$14+i$
1	2	0	7
1	2	1	$11+2i$
1	3	0	$8+3i$
1	3	1	$18+3i$
2	0	0	9
2	0	1	$13+2i$
2	1	0	$16+i$
2	1	1	$6+i$
2	2	0	19
2	2	1	$3+2i$
2	3	0	$3i$
2	3	1	$10+3i$
3	0	0	13
3	0	1	$17+2i$
3	1	0	i
3	1	1	$10+i$
3	2	0	3
3	2	1	$7+2i$
3	3	0	$4+3i$
3	3	1	$14+3i$
(4)	(4)	(2)	

i	3	1	0
$3i$	2	3	0
1	0	0	0
$1+2i$	1	0	1
$2+3i$	0	3	1
3	3	2	0
$3+2i$	2	2	1
$4+i$	1	1	0
$4+3i$	3	3	0
$5+2i$	0	0	1
$6+i$	2	1	1
7	1	2	0
$7+2i$	3	2	1
$8+i$	0	1	0
$8+3i$	1	3	0
9	2	0	0
$10+i$	3	1	1
$10+3i$	2	3	1
11	0	2	0
$11+2i$	1	2	1
$12+3i$	0	3	0
13	3	0	0
$13+2i$	2	0	1
$14+i$	1	1	1
$14+3i$	3	3	1
$15+2i$	0	2	1
$16+i$	2	1	0
17	1	0	0
$17+2i$	3	0	1
$18+i$	0	1	1
$18+3i$	1	3	1
19	2	2	0
	(4)	(4)	(2)

$$m = 4 + 8i = -(1+i)^4(1+2i) \quad \mathrm{N}(m) = 80 \quad \Phi(m) = 32 = 2.2^2.2^3 \quad \mathrm{H.E.} = 4$$

$$y \equiv \mathrm{Y} \pmod{4} \quad x \equiv \mathrm{X} + 17(\mathrm{Y} - y) \pmod{20}.$$

Generators 17, $3i$, $17 + 2i$.

0	0	0	1
0	0	1	$17+2i$
0	1	0	$3i$
0	1	1	$10+3i$
0	2	0	11
0	2	1	$7+2i$
0	3	0	$4+i$
0	3	1	$14+i$
1	0	0	17
1	0	1	$13+2i$
1	1	0	$16+3i$
1	1	1	$6+3i$
1	2	0	7
1	2	1	$3+2i$
1	3	0	i
1	3	1	$10+i$
2	0	0	9
2	0	1	$5+2i$
2	1	0	$8+3i$
2	1	1	$18+3i$
2	2	0	19
2	2	1	$15+2i$
2	3	0	$12+i$
2	3	1	$2+i$
3	0	0	13
3	0	1	$9+2i$
3	1	0	$12+3i$
3	1	1	$2+3i$
3	2	0	3
3	2	1	$19+2i$
3	3	0	$16+i$
3	3	1	$6+i$
(4)	(4)	(2)	

i	1	3	0
$3i$	0	1	0
1	0	0	0
$2+i$	2	3	1
$2+3i$	3	1	1
3	3	2	0
$3+2i$	1	2	1
$4+i$	0	3	0
$5+2i$	2	0	1
$6+i$	3	3	1
$6+3i$	1	1	1
7	1	2	0
$7+2i$	0	2	1
$8+3i$	2	1	0
9	2	0	0
$9+2i$	3	0	1
$10+i$	1	3	1
$10+3i$	0	1	1
11	0	2	0
$12+i$	2	3	0
$12+3i$	3	1	0
13	3	0	0
$13+2i$	1	0	1
$14+i$	0	3	1
$15+2i$	2	2	1
$16+i$	3	3	0
$16+3i$	1	1	0
17	1	0	0
$17+2i$	0	0	1
$18+3i$	2	1	1
19	2	2	0
$19+2i$	3	2	1
	(4)	(4)	(2)

$$m = 9 = 3^2 \quad \mathrm{N}\,(m) = 81 \quad \Phi\,(m) = 72 = 2^3.\ 3.\ 3 \quad \mathrm{H.\,E.} = 24$$

$$x \equiv \mathrm{X}\ (\mathrm{mod}\ 9) \quad y \equiv \mathrm{Y}\ (\mathrm{mod}\ 9).$$

Generators $2 + i$, $4 + 3i$.

0	0	1	8	0	$4+6i$	16	0	$7+3i$
0	1	$4+3i$	8	1	7	16	1	$1+6i$
0	2	$7+6i$	8	2	$1+3i$	16	2	4
1	0	$2+i$	9	0	$2+7i$	17	0	$2+4i$
1	1	$5+i$	9	1	$5+7i$	17	1	$5+4i$
1	2	$8+i$	9	2	$8+7i$	17	2	$8+4i$
2	0	$3+4i$	10	0	$6+7i$	18	0	i
2	1	$7i$	10	1	$3+i$	18	1	$6+4i$
2	2	$6+i$	10	2	$4i$	18	2	$3+7i$
3	0	$2+2i$	11	0	$5+2i$	19	0	$8+2i$
3	1	$2+5i$	11	1	$5+5i$	19	1	$8+5i$
3	2	$2+8i$	11	2	$5+8i$	19	2	$8+8i$
4	0	$2+6i$	12	0	8	20	0	$5+3i$
4	1	$8+3i$	12	1	$5+6i$	20	1	2
4	2	5	12	2	$2+3i$	20	2	$8+6i$
5	0	$7+5i$	13	0	$7+8i$	21	0	$7+2i$
5	1	$4+5i$	13	1	$4+8i$	21	1	$4+2i$
5	2	$1+5i$	13	2	$1+8i$	21	2	$1+2i$
6	0	$8i$	14	0	$6+5i$	22	0	$3+2i$
6	1	$3+5i$	14	1	$2i$	22	1	$6+8i$
6	2	$6+2i$	14	2	$3+8i$	22	2	$5i$
7	0	$1+7i$	15	0	$7+7i$	23	0	$4+7i$
7	1	$1+4i$	15	1	$7+4i$	23	1	$4+4i$
7	2	$1+i$	15	2	$7+i$	23	2	$4+i$
(24)	(3)		(24)	(3)		(24)	(3)	

i	18	0	$3+i$	10	1	$6+i$	2	2
$2i$	14	1	$3+2i$	22	0	$6+2i$	6	2
$4i$	10	2	$3+4i$	2	0	$6+4i$	18	1
$5i$	22	2	$3+5i$	6	1	$6+5i$	14	0
$7i$	2	1	$3+7i$	18	2	$6+7i$	10	0
$8i$	6	0	$3+8i$	14	2	$6+8i$	22	1
1	0	0	4	16	2	7	8	1
$1+i$	7	2	$4+i$	23	2	$7+i$	15	2
$1+2i$	21	2	$4+2i$	21	1	$7+2i$	21	0
$1+3i$	8	2	$4+3i$	0	1	$7+3i$	16	0
$1+4i$	7	1	$4+4i$	23	1	$7+4i$	15	1
$1+5i$	5	2	$4+5i$	5	1	$7+5i$	5	0
$1+6i$	16	1	$4+6i$	8	0	$7+6i$	0	2
$1+7i$	7	0	$4+7i$	23	0	$7+7i$	15	0
$1+8i$	13	2	$4+8i$	13	1	$7+8i$	13	0
2	20	1	5	4	2	8	12	0
$2+i$	1	0	$5+i$	1	1	$8+i$	1	2
$2+2i$	3	0	$5+2i$	11	0	$8+2i$	19	0
$2+3i$	12	2	$5+3i$	20	0	$8+3i$	4	1
$2+4i$	17	0	$5+4i$	17	1	$8+4i$	17	2
$2+5i$	3	1	$5+5i$	11	1	$8+5i$	19	1
$2+6i$	4	0	$5+6i$	12	1	$8+6i$	20	2
$2+7i$	9	0	$5+7i$	9	1	$8+7i$	9	2
$2+8i$	3	2	$5+8i$	11	2	$8+8i$	19	2
	(24)	(3)		(24)	(3)		(24)	(3)

$$m = 9 + i = - i(1 + i)(4 + 5i) \quad \mathrm{N}(m) = 82 \quad \Phi(m) = 40 = 2^3 . 5$$

$$\text{H. E.} = 40 \quad x \equiv \mathrm{X} + 73\mathrm{Y} \pmod{82}.$$

$$m = 1 + 9i = (1 + i)(5 + 4i) \quad \mathrm{N}(m) = 82 \quad \Phi(m) = 40 = 2^3 . 5$$

$$\text{H. E.} \equiv 40 \quad x \equiv \mathrm{X} + 9\mathrm{Y} \pmod{82}.$$

Generator 7.

I	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	(40)
N	1	7	49	15	23	79	61	17	37	13	9	63	31	53	43	55	57	71	5	35	
I	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	(40)
N	81	75	33	67	59	3	21	65	45	69	73	19	51	29	39	27	25	11	77	47	

N	1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39	
I	0	25	18	1	10	37	9	3	7	31	26	4	36	35	33	12	22	19	8	34	(40)
N	43	45	47	49	51	53	55	57	59	61	63	65	67	69	71	73	75	77	79	81	
I	14	28	39	2	32	13	15	16	24	6	11	27	23	29	17	30	21	38	5	20	(40)

$$m = 9 + 2i = -i(2+i)(1+4i) \quad 2 + 9i = (1+2i)(4+i) \quad 7 + 6i = (2+i)(4+i)$$
$$\text{or } 6 + 7i = -i(1+2i)(1+4i).$$

For all $N(m) = 85 \quad \Phi(m) = 64 = 2^2 . 2^4 \quad$ H.E. $= 16$.

$$m = 9 + 2i \quad x \equiv X + 38Y \pmod{85} \quad m = 2 + 9i \quad x \equiv X + 47Y \pmod{85}$$
$$m = 7 + 6i \quad x \equiv X + 13Y \pmod{85} \quad m = 6 + 7i \quad x \equiv X + 72Y \pmod{85}.$$

Generators 3, 52.

0	0	1
0	1	52
0	2	69
0	3	18
1	0	3
1	1	71
1	2	37
1	3	54
2	0	9
2	1	43
2	2	26
2	3	77
3	0	27
3	1	44
3	2	78
3	3	61
4	0	81
4	1	47
4	2	64
4	3	13
5	0	73
5	1	56
5	2	22
5	3	39
6	0	49
6	1	83
6	2	66
6	3	32
7	0	62
7	1	79
7	2	28
7	3	11
(16)	(4)	

8	0	16
8	1	67
8	2	84
8	3	33
9	0	48
9	1	31
9	2	82
9	3	14
10	0	59
10	1	8
10	2	76
10	3	42
11	0	7
11	1	24
11	2	58
11	3	41
12	0	21
12	1	72
12	2	4
12	3	38
13	0	63
13	1	46
13	2	12
13	3	29
14	0	19
14	1	53
14	2	36
14	3	2
15	0	57
15	1	74
15	2	23
15	3	6
(16)	(4)	

1	0	0
2	14	3
3	1	0
4	12	2
6	15	3
7	11	0
8	10	1
9	2	0
11	7	3
12	13	2
13	4	3
14	9	3
16	8	0
18	0	3
19	14	0
21	12	0
22	5	2
23	15	2
24	11	1
26	2	2
27	3	0
28	7	2
29	13	3
31	9	1
32	6	3
33	8	3
36	14	2
37	1	2
38	12	3
39	5	3
41	11	3
42	10	3
	(16)	(4)

43	2	1
44	3	1
46	13	1
47	4	1
48	9	0
49	6	0
52	0	1
53	14	1
54	1	3
56	5	1
57	15	0
58	11	2
59	10	0
61	3	3
62	7	0
63	13	0
64	4	2
66	6	2
67	8	1
69	0	2
71	1	1
72	12	1
73	5	0
74	15	1
76	10	2
77	2	3
78	3	2
79	7	1
81	4	0
82	9	2
83	6	1
84	8	2
	(16)	(4)

$m = 8 + 5i \quad \mathrm{N}(m) = 89 \quad \Phi(m) = 88 = 2^3.11 \quad \mathrm{H.E.} = 88 \quad x \equiv \mathrm{X} + 34\,\mathrm{Y} \pmod{89}.$

$m = 5 + 8i \quad \mathrm{N}(m) = 89 \quad \Phi(m) = 88 = 2^3.11 \quad \mathrm{H.E.} = 88 \quad x \equiv \mathrm{X} + 55\,\mathrm{Y} \pmod{89}.$

Generator 3.

I	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	(88)
N	1	3	9	27	81	65	17	51	64	14	42	37	22	66	20	60	2	6	18	54	73	41	
I	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	(88)
N	34	13	39	28	84	74	44	43	40	31	4	12	36	19	57	82	68	26	78	56	79	59	
I	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	(88)
N	88	86	80	62	8	24	72	38	25	75	47	52	67	23	69	29	87	83	71	35	16	48	
I	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	(88)
N	55	76	50	61	5	15	45	46	49	58	85	77	53	70	32	7	21	63	11	33	10	30	

N	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	
I	0	16	1	32	70	17	81	48	2	86	84	33	23	9	71	64	6	18	35	14	82	12	(88)
N	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	
I	57	49	52	39	3	25	59	87	31	80	85	22	63	34	11	51	24	30	21	10	29	28	(88)
N	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	
I	72	73	54	65	74	68	7	55	78	19	66	41	36	75	43	15	69	47	83	8	5	13	(88)
N	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	
I	56	38	58	79	62	50	20	27	53	67	77	40	42	46	4	37	61	26	76	45	60	44	(88)

$$m = 9 + 3i = -i\,(1 + i)\,(1 + 2i)\,3 \quad \mathrm{N}\,(m) = 90 \quad \Phi\,(m) = 32 = 2^2 . 2^3$$

$$\mathrm{H. E.} = 8 \quad y \equiv \mathrm{Y} \pmod 3 \quad x \equiv \mathrm{X} + 7\,(\mathrm{Y} - y) \pmod{30}.$$

Generators $2 + i$, i.

0	0	1
0	1	i
0	2	29
0	3	$9+2i$
1	0	$2+i$
1	1	$29+2i$
1	2	$7+2i$
1	3	$10+i$
2	0	$24+i$
2	1	17
2	2	$15+2i$
2	3	13
3	0	$5+2i$
3	1	$19+2i$
3	2	$4+i$
3	3	$20+i$
4	0	11
4	1	$3+2i$
4	2	19
4	3	$6+i$
5	0	$25+2i$
5	1	$16+i$
5	2	$14+i$
5	3	$23+2i$
6	0	$27+2i$
6	1	7
6	2	$12+i$
6	3	23
7	0	$22+i$
7	1	$26+i$
7	2	$17+2i$
7	3	$13+2i$
(8)	(4)	

i	0	1
1	0	0
$2+i$	1	0
$3+2i$	4	1
$4+i$	3	2
$5+2i$	3	0
$6+i$	4	3
7	6	1
$7+2i$	1	2
$9+2i$	0	3
$10+i$	1	3
11	4	0
$12+i$	6	2
13	2	3
$13+2i$	7	3
$14+i$	5	2
$15+2i$	2	2
$16+i$	5	1
17	2	1
$17+2i$	7	2
19	4	2
$19+2i$	3	1
$20+i$	3	3
$22+i$	7	0
23	6	3
$23+2i$	5	3
$24+i$	2	0
$25+2i$	5	0
$26+i$	7	1
$27+2i$	6	0
29	0	2
$29+2i$	1	1
	(8)	(4)

$$m = 3 + 9i = (1 + i)(2 + i)\,3 \quad \mathrm{N}(m) = 90 \quad \Phi(m) = 32 = 2^2.\,2^3$$

$$\mathrm{H.E.} = 8 \quad y \equiv \mathrm{Y} \pmod 3 \quad x \equiv \mathrm{X} + 23(\mathrm{Y} - y) \pmod{30}.$$

Generators $23 + 2i$, $21 + 2i$.

0	0	1
0	1	$21+2i$
0	2	29
0	3	i
1	0	$23+2i$
1	1	$20+i$
1	2	$28+i$
1	3	$1+2i$
2	0	$15+2i$
2	1	17
2	2	$6+i$
2	3	13
3	0	$26+i$
3	1	$10+i$
3	2	$25+2i$
3	3	$11+2i$
4	0	11
4	1	$24+i$
4	2	19
4	3	$27+2i$
5	0	$16+i$
5	1	$7+2i$
5	2	$5+2i$
5	3	$14+i$
6	0	$18+i$
6	1	7
6	2	$3+2i$
6	3	23
7	0	$13+2i$
7	1	$17+2i$
7	2	$8+i$
7	3	$4+i$
(8)	(4)	

i	0	3
1	0	0
$1+2i$	1	3
$3+2i$	6	2
$4+i$	7	3
$5+2i$	5	2
$6+i$	2	2
7	6	1
$7+2i$	5	1
$8+i$	7	2
$10+i$	3	1
11	4	0
$11+2i$	3	3
13	2	3
$13+2i$	7	0
$14+i$	5	3
$15+2i$	2	0
$16+i$	5	0
17	2	1
$17+2i$	7	1
$18+i$	6	0
19	4	2
$20+i$	1	1
$21+2i$	0	1
23	6	3
$23+2i$	1	0
$24+i$	4	1
$25+2i$	3	2
$26+i$	3	0
$27+2i$	4	3
$28+i$	1	2
29	0	2
	(8)	(4)

$m = 9 + 4i$ $\quad N(m) = 97$ $\quad \Phi(m) = 96 = 2^5 . 3$ $\quad$ H. E. $= 96$ $\quad x \equiv X + 22Y \pmod{97}$.

$m = 4 + 9i$ $\quad N(m) = 97$ $\quad \Phi(m) = 96 = 2^5 . 3$ $\quad$ H. E. $= 96$ $\quad x \equiv X + 75Y \pmod{97}$.

Generator 5.

I	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	(96)
N	1	5	25	28	43	21	8	40	6	30	53	71	64	29	48	46	36	83	27	38	
I	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38		(96)
N	93	77	94	82	22	13	65	34	73	74	79	7	35	78	2	10	50	56	86		
I	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57		(96)
N	42	16	80	12	60	9	45	31	58	96	92	72	69	54	76	89	57	91	67		
I	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76		(96)
N	44	26	33	68	49	51	61	14	70	59	4	20	3	15	75	84	32	63	24		
I	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95		(96)
N	23	18	90	62	19	95	87	47	41	11	55	81	17	85	37	88	52	66	39		

N	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	
I	0	34	70	68	1	8	31	6	44	35	86	42	25	65	71	40	89	78	81	69	(96)
N	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39		
I	5	24	77	76	2	59	18	3	13	9	46	74	60	27	32	16	91	19	95		(96)
N	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58		
I	7	85	39	4	58	45	15	84	14	62	36	63	93	10	52	87	37	55	47		(96)
N	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77		
I	67	43	64	80	75	12	26	94	57	61	51	66	11	50	28	29	72	53	21		(96)
N	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96		
I	33	30	41	88	23	17	73	90	38	83	92	54	79	56	49	20	22	82	48		(96)

$$m = 7 + 7i = (1 + i)\,7 \quad \mathrm{N}\,(m) = 98 \quad \Phi\,(m) = 48 = 2^4 .\, 3 \quad \mathrm{H.\ E.} = 48$$

$$y \equiv \mathbf{Y} \pmod{7} \quad x \equiv \mathrm{X} + \mathrm{Y} - y \pmod{14}.$$

Generator $2 + i$.

0	1
1	$2+i$
2	$3+4i$
3	$9+4i$
4	$3i$
5	$11+6i$
6	$9+2i$
7	$9+6i$
8	5
9	$10+5i$
10	$1+6i$
11	$3+6i$
12	i
13	$13+2i$
14	$10+3i$
15	$3+2i$
16	11
17	$1+4i$
18	$5+2i$
19	$1+2i$
20	$5i$
21	$2+3i$
22	$8+i$
23	$8+3i$

(48)

24	13
25	$5+6i$
26	$4+3i$
27	$12+3i$
28	$7+4i$
29	$10+i$
30	$12+5i$
31	$12+i$
32	9
33	$11+2i$
34	$6+i$
35	$4+i$
36	$7+6i$
37	$8+5i$
38	$11+4i$
39	$4+5i$
40	3
41	$6+3i$
42	$2+5i$
43	$6+5i$
44	$7+2i$
45	$5+4i$
46	$13+6i$
47	$13+4i$

(48)

i	12
$3i$	4
$5i$	20
1	0
$1+2i$	19
$1+4i$	17
$1+6i$	10
$2+i$	1
$2+3i$	21
$2+5i$	42
3	40
$3+2i$	15
$3+4i$	2
$3+6i$	11
$4+i$	35
$4+3i$	26
$4+5i$	39
5	8
$5+2i$	18
$5+4i$	45
$5+6i$	25
$6+i$	34
$6+3i$	41
$6+5i$	43

(48)

$7+2i$	44
$7+4i$	28
$7+6i$	36
$8+i$	22
$8+3i$	23
$8+5i$	37
9	32
$9+2i$	6
$9+4i$	3
$9+6i$	7
$10+i$	29
$10+3i$	14
$10+5i$	9
11	16
$11+2i$	33
$11+4i$	38
$11+6i$	5
$12+i$	31
$12+3i$	27
$12+5i$	30
13	24
$13+2i$	13
$13+4i$	47
$13+6i$	46

(48)

$$m = 8 + 6i = -(1+i)^2(1+2i)^2 \quad \mathrm{N}(m) = 100 \quad \Phi(m) = 40 = 2.2^2.5.$$

$$\text{H. E.} = 20 \quad y \equiv \mathrm{Y} \pmod{2} \quad x \equiv \mathrm{X} + 7(\mathrm{Y} - y) \pmod{50}.$$

Generators 3, $44 + i$.

0	0	1
0	1	$44+i$
1	0	3
1	1	$46+i$
2	0	9
2	1	$2+i$
3	0	27
3	1	$20+i$
4	0	31
4	1	$24+i$
5	0	43
5	1	$36+i$
6	0	29
6	1	$22+i$
7	0	37
7	1	$30+i$
8	0	11
8	1	$4+i$
9	0	33
9	1	$26+i$
(20)	(2)	

10	0	49
10	1	$42+i$
11	0	47
11	1	$40+i$
12	0	41
12	1	$34+i$
13	0	23
13	1	$16+i$
14	0	19
14	1	$12+i$
15	0	7
15	1	i
16	0	21
16	1	$14+i$
17	0	13
17	1	$6+i$
18	0	39
18	1	$32+i$
19	0	17
19	1	$10+i$
(20)	(2)	

i	15	1
1	0	0
$2+i$	2	1
3	1	0
$4+i$	8	1
$6+i$	17	1
7	15	0
9	2	0
$10+i$	19	1
11	8	0
$12+i$	14	1
13	17	0
$14+i$	16	1
$16+i$	13	1
17	19	0
19	14	0
$20+i$	3	1
21	16	0
$22+i$	6	1
23	13	0
	(20)	(2)

$24+i$	4	1
$26+i$	9	1
27	3	0
29	6	0
$30+i$	7	1
31	4	0
$32+i$	18	1
33	9	0
$34+i$	12	1
$36+i$	5	1
37	7	0
39	18	0
$40+i$	11	1
41	12	0
$42+i$	10	1
43	5	0
$44+i$	0	1
$46+i$	1	1
47	11	0
49	10	0
	(20)	(2)

$$m = 6 + 8i = -i(1+i)^2(2+i)^2 \quad \mathrm{N}(m) = 100 \quad \Phi(m) = 40 = 2.2^2.5$$

$$\text{H. E.} = 20 \quad y \equiv \mathrm{Y} \pmod{2} \quad x \equiv \mathrm{X} + 43(\mathrm{Y} - y) \pmod{50}.$$

Generators 3, $8 + i$.

0	0	1
0	1	$8+i$
1	0	3
1	1	$10+i$
2	0	9
2	1	$16+i$
3	0	27
3	1	$34+i$
4	0	31
4	1	$38+i$
5	0	43
5	1	i
6	0	29
6	1	$36+i$
7	0	37
7	1	$44+i$
8	0	11
8	1	$18+i$
9	0	33
9	1	$40+i$
(20)	(2)	

10	0	49
10	1	$6+i$
11	0	47
11	1	$4+i$
12	0	41
12	1	$48+i$
13	0	23
13	1	$30+i$
14	0	19
14	1	$26+i$
15	0	7
15	1	$14+i$
16	0	21
16	1	$28+i$
17	0	13
17	1	$20+i$
18	0	39
18	1	$46+i$
19	0	17
19	1	$24+i$
(20)	(2)	

i	5	1
1	0	0
3	1	0
$4+i$	11	1
$6+i$	10	1
7	15	0
$8+i$	0	1
9	2	0
$10+i$	1	1
11	8	0
13	17	0
$14+i$	15	1
$16+i$	2	1
17	19	0
$18+i$	8	1
19	14	0
$20+i$	17	1
21	16	0
23	13	0
$24+i$	19	1
	(20)	(2)

$26+i$	14	1
27	3	0
$28+i$	16	1
29	6	0
$30+i$	13	1
31	4	0
33	9	0
$34+i$	3	1
$36+i$	6	1
37	7	0
$38+i$	4	1
39	18	0
$40+i$	9	1
41	12	0
43	5	0
$44+i$	7	1
$46+i$	18	1
47	11	0
$48+i$	12	1
49	10	0
	(20)	(2)

$$m = 10 = -(1+i)^2(1+2i)(2+i) \quad \mathrm{N}(m) = 100 \quad \Phi(m) = 32 = 2.2^2.2^2. \quad \text{H. E.} = 4$$

$$x \equiv \mathrm{X} \pmod{10} \quad y \equiv \mathrm{Y} \pmod{10}.$$

Generators $9+4i$, $9+6i$, $6+5i$.

0	0	0	1
0	0	1	$6+5i$
0	1	0	$9+6i$
0	1	1	$4+i$
0	2	0	$5+8i$
0	2	1	$3i$
0	3	0	$7+2i$
0	3	1	$2+7i$
1	0	0	$9+4i$
1	0	1	$4+9i$
1	1	0	7
1	1	1	$2+5i$
1	2	0	$3+2i$
1	2	1	$8+7i$
1	3	0	$5+6i$
1	3	1	i
2	0	0	$5+2i$
2	0	1	$7i$
2	1	0	$3+8i$
2	1	1	$8+3i$
2	2	0	9
2	2	1	$4+5i$
2	3	0	$1+4i$
2	3	1	$6+9i$
3	0	0	$7+8i$
3	0	1	$2+3i$
3	1	0	$5+4i$
3	1	1	$9i$
3	2	0	$1+6i$
3	2	1	$6+i$
3	3	0	3
3	3	1	$8+5i$
(4)	(4)	(2)	

i	1	3	1
$3i$	0	2	1
$7i$	2	0	1
$9i$	3	1	1
1	0	0	0
$1+4i$	2	3	0
$1+6i$	3	2	0
$2+3i$	3	0	1
$2+5i$	1	1	1
$2+7i$	0	3	1
3	3	3	0
$3+2i$	1	2	0
$3+8i$	2	1	0
$4+i$	0	1	1
$4+5i$	2	2	1
$4+9i$	1	0	1
$5+2i$	2	0	0
$5+4i$	3	1	0
$5+6i$	1	3	0
$5+8i$	0	2	0
$6+i$	3	2	1
$6+5i$	0	0	1
$6+9i$	2	3	1
7	1	1	0
$7+2i$	0	3	0
$7+8i$	3	0	0
$8+3i$	2	1	1
$8+5i$	3	3	1
$8+7i$	1	2	1
9	2	2	0
$9+4i$	1	0	0
$9+6i$	0	1	0
	(4)	(4)	(2)

Mod $(1 + i)$.

1	1

Mod $(1 + i)^2$.

Generator i.

i	1
1	0
	(2)

Mod $(1 + i)^3$.

Generator i.

i	1
3	2
$2+i$	3
1	0
	(4)

Mod $(1 + i)^4$

Generators i, $1 + 2i$.

0	0	1
0	1	$1+2i$
1	0	i
1	1	$2+i$
2	0	3
2	1	$3+2i$
3	0	$3i$
3	1	$2+3i$
(4)	(2)	

i	1	0
$3i$	3	0
1	0	0
$1+2i$	0	1
$2+i$	1	1
$2+3i$	3	1
3	2	0
$3+2i$	2	1
	(4)	(2)

Mod $(1 + i)^5$.

Generators i, $1 + 2i$, 3.

0	0	0	1
0	0	1	3
0	1	0	$1+2i$
0	1	1	$7+2i$
1	0	0	i
1	0	1	$3i$
1	1	0	$6+i$
1	1	1	$2+3i$
2	0	0	7
2	0	1	5
2	1	0	$3+2i$
2	1	1	$5+2i$
3	0	0	$4+3i$
3	0	1	$4+i$
3	1	0	$6+3i$
3	1	1	$2+i$
(4)	(2)	(2)	

i	1	0	0
$3i$	1	0	1
1	0	0	0
$1+2i$	0	1	0
$2+i$	3	1	1
$2+3i$	1	1	1
3	0	0	1
$3+2i$	2	1	0
$4+i$	3	0	1
$4+3i$	3	0	0
5	2	0	1
$5+2i$	2	1	1
$6+i$	1	1	0
$6+3i$	3	1	0
7	2	0	0
$7+2i$	0	1	1
	(4)	(2)	(2)

Mod $(1 + i)^6$.

Generators i, $1 + 2i$, 3.

0	0	0	1
0	0	1	3
0	1	0	$1+2i$
0	1	1	$3+6i$
0	2	0	$5+4i$
0	2	1	$7+4i$
0	3	0	$5+6i$
0	3	1	$7+2i$
1	0	0	i
1	0	1	$3i$
1	1	0	$6+i$
1	1	1	$2+3i$
1	2	0	$4+5i$
1	2	1	$4+7i$
1	3	0	$2+5i$
1	3	1	$6+7i$
2	0	0	7
2	0	1	5
2	1	0	$7+6i$
2	1	1	$5+2i$
2	2	0	$3+4i$
2	2	1	$1+4i$
2	3	0	$3+2i$
2	3	1	$1+6i$
3	0	0	$7i$
3	0	1	$5i$
3	1	0	$2+7i$
3	1	1	$6+5i$
3	2	0	$4+3i$
3	2	1	$4+i$
3	3	0	$6+3i$
3	3	1	$2+i$
(4)	(4)	(2)	

i	1	0	0
$3i$	1	0	1
$5i$	3	0	1
$7i$	3	0	0
1	0	0	0
$1+2i$	0	1	0
$1+4i$	2	1	1
$1+6i$	2	3	1
$2+i$	3	3	1
$2+3i$	1	1	1
$2+5i$	1	3	0
$2+7i$	3	1	0
3	0	0	1
$3+2i$	2	3	0
$3+4i$	2	2	0
$3+6i$	0	1	1
$4+i$	3	2	1
$4+3i$	3	2	0
$4+5i$	1	2	0
$4+7i$	1	2	1
5	2	0	1
$5+2i$	2	1	1
$5+4i$	0	2	0
$5+6i$	0	3	0
$6+i$	1	1	0
$6+3i$	3	3	0
$6+5i$	3	1	1
$6+7i$	1	3	1
7	2	0	0
$7+2i$	0	3	1
$7+4i$	0	2	1
$7+6i$	2	1	0
	(4)	(4)	(2)

Mod $(1+i)^7$.

Generators i, 3, $1+2i$.

0	0	0	1	2	0	0	15
0	0	1	$1+2i$	2	0	1	$7+6i$
0	0	2	$13+4i$	2	0	2	$11+4i$
0	0	3	$13+6i$	2	0	3	$11+2i$
0	1	0	3	2	1	0	13
0	1	1	$3+6i$	2	1	1	$5+2i$
0	1	2	$15+4i$	2	1	2	$9+4i$
0	1	3	$7+2i$	2	1	3	$1+6i$
0	2	0	9	2	2	0	7
0	2	1	$9+2i$	2	2	1	$15+6i$
0	2	2	$5+4i$	2	2	2	$3+4i$
0	2	3	$5+6i$	2	2	3	$3+2i$
0	3	0	11	2	3	0	5
0	3	1	$11+6i$	2	3	1	$13+2i$
0	3	2	$7+4i$	2	3	2	$1+4i$
0	3	3	$15+2i$	2	3	3	$9+6i$
1	0	0	i	3	0	0	$8+7i$
1	0	1	$14+i$	3	0	1	$10+7i$
1	0	2	$4+5i$	3	0	2	$4+3i$
1	0	3	$2+5i$	3	0	3	$6+3i$
1	1	0	$3i$	3	1	0	$8+5i$
1	1	1	$10+3i$	3	1	1	$14+5i$
1	1	2	$4+7i$	3	1	2	$4+i$
1	1	3	$14+7i$	3	1	3	$10+i$
1	2	0	$8+i$	3	2	0	$7i$
1	2	1	$6+i$	3	2	1	$2+7i$
1	2	2	$12+5i$	3	2	2	$12+3i$
1	2	3	$10+5i$	3	2	3	$14+3i$
1	3	0	$8+3i$	3	3	0	$5i$
1	3	1	$2+3i$	3	3	1	$6+5i$
1	3	2	$12+7i$	3	3	2	$12+i$
1	3	3	$6+7i$	3	3	3	$2+i$
(4)	(4)	(4)		(4)	(4)	(4)	

i	1	0	0	$8+i$	1	2	0
$3i$	1	1	0	$8+3i$	1	3	0
$5i$	3	3	0	$8+5i$	3	1	0
$7i$	3	2	0	$8+7i$	3	0	0
1	0	0	0	9	0	2	0
$1+2i$	0	0	1	$9+2i$	0	2	1
$1+4i$	2	3	2	$9+4i$	2	1	2
$1+6i$	2	1	3	$9+6i$	2	3	3
$2+i$	3	3	3	$10+i$	3	1	3
$2+3i$	1	3	1	$10+3i$	1	1	1
$2+5i$	1	0	3	$10+5i$	1	2	3
$2+7i$	3	2	1	$10+7i$	3	0	1
3	0	1	0	11	0	3	0
$3+2i$	2	2	3	$11+2i$	2	0	3
$3+4i$	2	2	2	$11+4i$	2	0	2
$3+6i$	0	1	1	$11+6i$	0	3	1
$4+i$	3	1	2	$12+i$	3	3	2
$4+3i$	3	0	2	$12+3i$	3	2	2
$4+5i$	1	0	2	$12+5i$	1	2	2
$4+7i$	1	1	2	$12+7i$	1	3	2
5	2	3	0	13	2	1	0
$5+2i$	2	1	1	$13+2i$	2	3	1
$5+4i$	0	2	2	$13+4i$	0	0	2
$5+6i$	0	2	3	$13+6i$	0	0	3
$6+i$	1	2	1	$14+i$	1	0	1
$6+3i$	3	0	3	$14+3i$	3	2	3
$6+5i$	3	3	1	$14+5i$	3	1	1
$6+7i$	1	3	3	$14+7i$	1	1	3
7	2	2	0	15	2	0	0
$7+2i$	0	1	3	$15+2i$	0	3	3
$7+4i$	0	3	2	$15+4i$	0	1	2
$7+6i$	2	0	1	$15+6i$	2	2	1
	(4)	(4)	(4)		(4)	(4)	(4)

Mod $(1+i)^8$.

Generators $1+2i$, 3, i.

0	0	0	1	2	0	0	$13+4i$	4	0	0	$9+8i$	6	0	0	$5+12i$
0	0	1	i	2	0	1	$12+13i$	4	0	1	$8+9i$	6	0	1	$4+5i$
0	0	2	15	2	0	2	$3+12i$	4	0	2	$7+8i$	6	0	2	$11+4i$
0	0	3	$15i$	2	0	3	$4+3i$	4	0	3	$8+7i$	6	0	3	$12+11i$
0	1	0	3	2	1	0	$7+12i$	4	1	0	$11+8i$	6	1	0	$15+4i$
0	1	1	$3i$	2	1	1	$4+7i$	4	1	1	$8+11i$	6	1	1	$12+15i$
0	1	2	13	2	1	2	$9+4i$	4	1	2	$5+8i$	6	1	2	$1+12i$
0	1	3	$13i$	2	1	3	$12+9i$	4	1	3	$8+5i$	6	1	3	$4+i$
0	2	0	9	2	2	0	$5+4i$	4	2	0	$1+8i$	6	2	0	$13+12i$
0	2	1	$9i$	2	2	1	$12+5i$	4	2	1	$8+i$	6	2	1	$4+13i$
0	2	2	7	2	2	2	$11+12i$	4	2	2	$15+8i$	6	2	2	$3+4i$
0	2	3	$7i$	2	2	3	$4+11i$	4	2	3	$8+15i$	6	2	3	$12+3i$
0	3	0	11	2	3	0	$15+12i$	4	3	0	$3+8i$	6	3	0	$7+4i$
0	3	1	$11i$	2	3	1	$4+15i$	4	3	1	$8+3i$	6	3	1	$12+7i$
0	3	2	5	2	3	2	$1+4i$	4	3	2	$13+8i$	6	3	2	$9+12i$
0	3	3	$5i$	2	3	3	$12+i$	4	3	3	$8+13i$	6	3	3	$4+9i$
1	0	0	$1+2i$	3	0	0	$5+14i$	5	0	0	$9+10i$	7	0	0	$13+6i$
1	0	1	$14+i$	3	0	1	$2+5i$	5	0	1	$6+9i$	7	0	1	$10+13i$
1	0	2	$15+14i$	3	0	2	$11+2i$	5	0	2	$7+6i$	7	0	2	$3+10i$
1	0	3	$2+15i$	3	0	3	$14+11i$	5	0	3	$10+7i$	7	0	3	$6+3i$
1	1	0	$3+6i$	3	1	0	$15+10i$	5	1	0	$11+14i$	7	1	0	$7+2i$
1	1	1	$10+3i$	3	1	1	$6+15i$	5	1	1	$2+11i$	7	1	1	$14+7i$
1	1	2	$13+10i$	3	1	2	$1+6i$	5	1	2	$5+2i$	7	1	2	$9+14i$
1	1	3	$6+13i$	3	1	3	$10+i$	5	1	3	$14+5i$	7	1	3	$2+9i$
1	2	0	$9+2i$	3	2	0	$13+14i$	5	2	0	$1+10i$	7	2	0	$5+6i$
1	2	1	$14+9i$	3	2	1	$2+13i$	5	2	1	$6+i$	7	2	1	$10+5i$
1	2	2	$7+14i$	3	2	2	$3+2i$	5	2	2	$15+6i$	7	2	2	$11+10i$
1	2	3	$2+7i$	3	2	3	$14+3i$	5	2	3	$10+15i$	7	2	3	$6+11i$
1	3	0	$11+6i$	3	3	0	$7+10i$	5	3	0	$3+14i$	7	3	0	$15+2i$
1	3	1	$10+11i$	3	3	1	$6+7i$	5	3	1	$2+3i$	7	3	1	$14+15i$
1	3	2	$5+10i$	3	3	2	$9+6i$	5	3	2	$13+2i$	7	3	2	$1+14i$
1	3	3	$6+5i$	3	3	3	$10+9i$	5	3	3	$14+13i$	7	3	3	$2+i$
(8)	(4)	(4)		(8)	(4)	(4)		(8)	(4)	(4)		(8)	(4)	(4)	

Mod $(1+i)^8$.

i	0	0	1	$4+i$	6	1	3	$8+i$	4	2	1	$12+i$	2	3	3
$3i$	0	1	1	$4+3i$	2	0	3	$8+3i$	4	3	1	$12+3i$	6	2	3
$5i$	0	3	3	$4+5i$	6	0	1	$8+5i$	4	1	3	$12+5i$	2	2	1
$7i$	0	2	3	$4+7i$	2	1	1	$8+7i$	4	0	3	$12+7i$	6	3	1
$9i$	0	2	1	$4+9i$	6	3	3	$8+9i$	4	0	1	$12+9i$	2	1	3
$11i$	0	3	1	$4+11i$	2	2	3	$8+11i$	4	1	1	$12+11i$	6	0	3
$13i$	0	1	3	$4+13i$	6	2	1	$8+13i$	4	3	3	$12+13i$	2	0	1
$15i$	0	0	3	$4+15i$	2	3	1	$8+15i$	4	2	3	$12+15i$	6	1	1
1	0	0	0	5	0	3	2	9	0	2	0	13	0	1	2
$1+2i$	1	0	0	$5+2i$	5	1	2	$9+2i$	1	2	0	$13+2i$	5	3	2
$1+4i$	2	3	2	$5+4i$	2	2	0	$9+4i$	2	1	2	$13+4i$	2	0	0
$1+6i$	3	1	2	$5+6i$	7	2	0	$9+6i$	3	3	2	$13+6i$	7	0	0
$1+8i$	4	2	0	$5+8i$	4	1	2	$9+8i$	4	0	0	$13+8i$	4	3	2
$1+10i$	5	2	0	$5+10i$	1	3	2	$9+10i$	5	0	0	$13+10i$	1	1	2
$1+12i$	6	1	2	$5+12i$	6	0	0	$9+12i$	6	3	2	$13+12i$	6	2	0
$1+14i$	7	3	2	$5+14i$	3	0	0	$9+14i$	7	1	2	$13+14i$	3	2	0
$2+i$	7	3	3	$6+i$	5	2	1	$10+i$	3	1	3	$14+i$	1	0	1
$2+3i$	5	3	1	$6+3i$	7	0	3	$10+3i$	1	1	1	$14+3i$	3	2	3
$2+5i$	3	0	1	$6+5i$	1	3	3	$10+5i$	7	2	1	$14+5i$	5	1	3
$2+7i$	1	2	3	$6+7i$	3	3	1	$10+7i$	5	0	3	$14+7i$	7	1	1
$2+9i$	7	1	3	$6+9i$	5	0	1	$10+9i$	3	3	3	$14+9i$	1	2	1
$2+11i$	5	1	1	$6+11i$	7	2	3	$10+11i$	1	3	1	$14+11i$	3	0	3
$2+13i$	3	2	1	$6+13i$	1	1	3	$10+13i$	7	0	1	$14+13i$	5	3	3
$2+15i$	1	0	3	$6+15i$	3	1	1	$10+15i$	5	2	3	$14+15i$	7	3	1
3	0	1	0	7	0	2	2	11	0	3	0	15	0	0	2
$3+2i$	3	2	2	$7+2i$	7	1	0	$11+2i$	3	0	2	$15+2i$	7	3	0
$3+4i$	6	2	2	$7+4i$	6	3	0	$11+4i$	6	0	2	$15+4i$	6	1	0
$3+6i$	1	1	0	$7+6i$	5	0	2	$11+6i$	1	3	0	$15+6i$	5	2	2
$3+8i$	4	3	0	$7+8i$	4	0	2	$11+8i$	4	1	0	$15+8i$	4	2	2
$3+10i$	7	0	2	$7+10i$	3	3	0	$11+10i$	7	2	2	$15+10i$	3	1	0
$3+12i$	2	0	2	$7+12i$	2	1	0	$11+12i$	2	2	2	$15+12i$	2	3	0
$3+14i$	5	3	0	$7+14i$	1	2	2	$11+14i$	5	1	0	$15+14i$	1	0	2
	(8)	(4)	(4)		(8)	(4)	(4)		(8)	(4)	(4)		(8)	(4)	(4)